Teoría de Conjuntos

(una introducción)

Fernando Hernández Hernández

Contenido

Prefacio **vii**

1 Introducción Histórica **1**

2 Axiomas de la Teoría de Conjuntos **7**
2.1 Propiedades 7
2.2 Los Axiomas 9

3 Álgebra de Conjuntos **23**
3.1 Operaciones Fundamentales 23
3.2 Producto Cartesiano 29
3.3 Familias de Conjuntos 34

4 Relaciones y Funciones **43**
4.1 Relaciones 43
4.2 Funciones 49
4.3 Productos Cartesianos Arbitrarios 63
4.4 Equivalencias y Particiones 69
4.5 Órdenes 77
4.6 Sobre Clases 92

5 Los Números Naturales **95**
5.1 Introducción 95
5.2 Propiedades de los Números Naturales 100
5.3 El Teorema de Recursión 105
5.4 Aritmética de los Números Naturales 111

6 La Extensión de los Naturales a los Reales **119**
6.1 Diferencias 119
6.2 Los Enteros 122
6.3 Los Racionales 126
6.4 Sucesiones de Cauchy de Números Racionales 132

6.5 Los Reales 138

7 Cardinalidad **149**
7.1 Introducción 149
7.2 Conjuntos Finitos 150
7.3 Cardinalidad en Conjuntos Infinitos 154
7.4 Conjuntos Numerables 156
7.5 Números Cardinales 161
7.6 Aritmética Cardinal 164
7.7 El Continuo 169

8 El Axioma de Elección **175**
8.1 Introducción 175
8.2 El Axioma de Elección 177
8.3 Cuatro Equivalencias Importantes 181
8.4 Uso del Axioma de Elección 188
8.5 El Teorema del Ideal Primo 199
8.6 Otras Proposiciones Relacionadas. 210
8.7 Matemáticas sin Elección. 214

9 Ordinales **217**
9.1 Introducción 217
9.2 Números Ordinales 218
9.3 El Axioma de Reemplazo 222
9.4 Inducción y Recursión Transfinita 227
9.5 Aritmética Ordinal 232
9.6 Ordinales Iniciales y Alephs 245
9.7 Suma y Multiplicación de Alephs 250

10 Teoría de Cardinales **255**
10.1 Números Cardinales y el Axioma de Elección 255
10.2 Sumas y Productos Infinitos 260
10.3 Cardinales Regulares y Singulares 266
10.4 La Hipótesis Generalizada del Continuo 271
10.5 La HGC y los Números Cardinales 275
10.6 Medidas y Cardinales 281
10.7 Cardinales Medibles 286
10.8 Otros Cardinales Grandes 288

11 Dos Tópicos Especiales **297**
11.1 El Problema de Souslin 297
11.2 El Axioma de Martin 301
11.3 Equivalencias del Axioma de Martin 312

A Axiomas de Zermelo-Fraenkel **319**

B Axiomas Bernays-Gödel **321**

C Axiomas Adicionales **323**

Bibliografía **329**

Índice **337**

Teoría de Conjuntos

Cada cuerpo tiene
su armonía y
su desarmonía

en algunos casos
la suma de armonías
puede ser casi
empalagosa

en otros
el conjunto
de desarmonías
produce algo mejor
que la belleza

Mario Benedetti

Viento del Exilio

Prefacio

Casi todos los libros de matemáticas hablan de conjuntos y están libremente salpicados de extraños símbolos como $\in$, $\subseteq$, $\cup$, $\cap$, $\emptyset$. P. R. Halmos apunta en el ya clásico *Naive Set Theory*: "Los matemáticos están de acuerdo en que cada uno de ellos debe saber algo de Teoría de Conjuntos; el desacuerdo comienza al tratar de decidir qué tanto es *algo"*. Hay motivos bien fundamentados detrás de esta obsesión por los conjuntos. La Teoría de Conjuntos es un lenguaje. Sin ella, no sólo es imposible hacer matemáticas, sino que ni siquiera podemos decir de qué se trata ésta. Es lo mismo que intentar estudiar literatura francesa sin saber algo de francés. Hewitt y Stromberg en su libro *Real and Abstract Analysis* dicen: "Desde el punto de vista de un lógico, las matemáticas son la Teoría de Conjuntos y sus consecuencias".

La Teoría Intuitiva de Conjuntos funciona bien para los primeros cursos de matemáticas (Cálculo, Álgebra, entre otros), pero definitivamente para los cursos de matemáticas superiores es muy conveniente contar con una Teoría de Conjuntos sólida pues, de hecho, nociones como las de cardinalidad o aplicaciones del Axioma de Elección son fundamentales y, en ocasiones, indispensables en tópicos especializados del Análisis, Álgebra, Topología, etc.

En este texto se presenta la Teoría de Conjuntos basada en la Axiomática de Zermelo-Fraenkel con elección (**ZFC**) tratando de requerir el mínimo de formalismo lógico. Una justificación para optar por la axiomatización de Zermelo-Fraenkel (**ZF**) es que ésta es la más apropiada para un primer encuentro con la Teoría de Conjuntos y lo más importante es que, como veremos, los números reales, sus operaciones aritméticas y las demostraciones de sus propiedades pueden ser expresados a partir de los axiomas de Zermelo-Fraenkel. Pero no sólo el sistema de los números reales encuentra sustento en la Axiomática de Zermelo-Fraenkel, la mayor parte de las matemáticas contemporáneas (posiblemente la única excepción es la Teoría de Categorías) puede desarrollarse dentro de la Teoría de Conjuntos así axiomatizada. Por ejemplo, los objetos fundamentales de Topología, Álgebra o Análisis (espacios topológicos, espacios vectoriales, grupos, anillos, espacios de Banach) son apropiadamente definidos como conjuntos de una clase específica. Propiedades topológicas, algebraicas o analíticas de estos objetos son entonces derivadas a

partir de las propiedades de conjuntos, las cuales se pueden obtener usando los axiomas **ZFC**. En este sentido, la Teoría de Conjuntos así axiomatizada sirve como una fundamentación satisfactoria para otras ramas de la matemática.

Una consulta rápida al contenido analítico será suficiente para enterarse de cuál es el material que se expone en este texto y cómo está organizado este material. Sin embargo, son convenientes algunos comentarios. En primer lugar, en el Capítulo 2, la noción de propiedad se da de manera intuitiva y se introducen los primeros axiomas del sistema **ZF**. En el Capítulo 6, la extensión de los números racionales a los números reales se hace estableciendo clases de equivalencia de sucesiones de Cauchy, en lugar del método clásico que utiliza cortaduras de Dedekind (que también se expone brevemente en el Capítulo 11). El Capítulo 8, que trata del Axioma de Elección, contiene mucha información, en especial, las Secciones 8.4 y 8.5 incluyen ejemplos que posiblemente no sean accesibles a todos los lectores; en particular, las demostraciones de éstos están destinadas a aquellos lectores con mayor conocimiento y madurez matemática. El propósito de incluir toda esta información es el de mostrar las vastas aplicaciones de dicho axioma en diversas áreas de la Matemática. La exposición del material dedicado a los números ordinales se pospone hasta después del Axioma de Elección por considerar a éste más importante, aunque por ello se sacrifique un poco el seguimiento de la exposición de los conceptos de cardinalidad; además de que es necesario dicho axioma en algunas proposiciones importantes que se refieren a números ordinales. El Capítulo 10 contiene tópicos especializados de Teoría de Cardinales y es deseable cubrir la mayor parte de él. Las dos últimas secciones de este capítulo requieren de los conceptos de ideales y filtros (para el caso especial del álgebra Booleana $\mathcal{P}(X)$) expuestos en la Sección 8.5. Por último, el Capítulo 11 puede considerarse optativo, el material que ahí se presenta es para aquellos lectores con mayor interés en la Teoría de Conjuntos o ramas afines como la Topología. Cabe mencionar que las secciones 11.2 y 11.3 están basadas en las notas de clase del curso sobre *forcing* que el Prof. Oleg G. Okunev impartió en la Facultad de Ciencias de la UNAM en el segundo semestre de 1997.

Por lo regular las secciones están seguidas de una lista de ejercicios. En pocas excepciones, los ejercicios no se refieren a los conceptos tratados en el texto. Hay varios tipos de ejercicios, algunos rutinarios y otros más difíciles, los cuales frecuentemente están acompañados con sugerencias para su solución. Los ejemplos en el texto sólo ocasionalmente son desarrollados con todo detalle. La verificación de que un ejemplo tiene las propiedades deseadas se deja como ejercicio (usualmente fácil) para el lector.

El final de una demostración se indica con el símbolo ■. Las definiciones, observaciones, lemas, proposiciones y teoremas de cada capítulo son numerados consecutivamente por un par de números que indican el capítulo y el elemento respectivamente: ver Lema 3.2, significa ver el Lema 2 del Capítulo 3. Para hacer referencia a los ejercicios usaremos una terna de números separados por puntos: Ejercicio 2.3.7, significa ejercicio 7 de la sección 3 del capítulo 2. Los axiomas se numeran consecutivamente a lo largo de todo el texto.

Hay referencias de carácter histórico, pero como es un poco incómodo poner todos los datos de la obra que se esté citando en el lugar donde se realizan los apuntes, en la bibliografía se encuentran algunas segundas referencias. Por otra parte, me parece oportuno indicar la bibliografía básica empleada en la elaboración del material aquí presentado, la cual está integrada por: [E_1], [H_1], [HJ], [J_3], [K_1], [KM], [P_4], [P_5], [R_2], [S_{10}]. A los autores de estos textos es a quien ha de atribuirse lo acertado de las demostraciones presentadas. El mérito (si existe) de este trabajo es la selección, modo de presentación del material, modificación y adaptación de algunas de las demostraciones.

La idea de escribir el presente trabajo tuvo su origen en las notas "Breve Resumen de Introducción a la Teoría de Conjuntos". En estas últimas se basó un seminario que realizamos algunos estudiantes de la Facultad de Ciencias Físico Matemáticas de la BUAP en 1992, el cual fue motivado por la falta de un curso de esta bella teoría. En los años en que han sido usadas las notas originales se observó que requerían de una revisión que las hiciera, hasta donde fuera posible, más entendibles y sobre todo más completas; así, el presente volumen difiere en mucho de las notas originales.

Es mi deseo que este libro sirva a cualquier interesado en las matemáticas; en especial a los estudiantes, para ayudarles a no sentirse confundidos (como en su momento yo lo estuve) por el concepto de conjunto.

Finalmente, y no por ello menos merecido, deseo manifestar mi sincero agradecimiento a todas las personas que de una u otra manera han colaborado en la realización de este libro y que por temor a aburrir al lector con una larga lista de nombres no citaré explícitamente. No obstante, es para mi un placer dar a conocer las personas que me ayudaron a culminar este trabajo y a quienes reitero mi agradecimiento: el Prof. Agustín Contreras Carreto, que pese a sus múltiples ocupaciones hizo un gran esfuerzo por brindarme su apreciable ayuda como el mejor de los amigos; el Prof. Fidel Casarrubias Segura, que me hizo observaciones muy acertadas sobre la manera en que se presentaba el material, que me estimuló en muchas ocasiones y que sobre todo me ha apoyado en tantos momentos difíciles; el Prof. Ángel Tamariz Mascarúa, cuya eficaz revisión mejoró notablemente la exposición del material

aquí presentado y de quien he recibido además de un muy especial apoyo, su confianza. Los comentarios constructivos y críticas de todos ellos fueron muy apreciados; además de que han influido de manera sustancial en la redacción final de este trabajo. Expreso también mi gratitud a mi esposa quien ha sufrido y soportado mis locuras desde que inicié con aquel proyecto de 1992 y que para culminar este trabajo me respaldó a pesar de sentirse desplazada. A mis padres por todo el apoyo y comprensión que de ellos he recibido.

Fernando Hernández Hernández.

1

Introducción Histórica

Puede decirse que en todas las épocas los matemáticos y filósofos han empleado razonamientos de la Teoría de Conjuntos de modo más o menos consciente. Sin embargo, es necesario separar claramente todas las cuestiones relacionadas con la idea de número cardinal (y en particular, la noción de infinito) de aquellas en las que solamente intervienen las nociones de pertenencia e inclusión pues éstas son más intuitivas. Solamente apoyándose en ellas es como se puede fundamentar una teoría de silogismos o axiomas como "el todo es mayor que cualquiera de sus partes".

Para la introducción de la Teoría de Conjuntos es muy útil trabajar con conjuntos concretos cuyos miembros sean objetos reales, pero los conjuntos de interés en matemáticas siempre tienen por miembros objetos abstractos: el conjunto de todos los círculos del plano, el conjunto de todos los puntos sobre una esfera, el conjunto de todos los números, etc.

A finales del siglo XIX ya no hay dificultad alguna en hablar del conjunto de los objetos que poseen tal o cual propiedad; la célebre "definición" dada por el matemático alemán Georg Ferdinand Ludwig Philipp Cantor (1845-1918)[1]:"*Se entiende por conjunto a la agrupación en un todo de objetos bien diferenciados de nuestra intuición o nuestra mente*", apenas despertó objeciones en el momento de su publicación. No sucedió así cuando a la noción de conjunto vinieron a unirse las de número y magnitud.

El problema de la divisibilidad de extensión da lugar a dificultades filosóficas considerables; matemáticos y filósofos fracasarían ante la paradoja[2] de una magnitud finita formada por infinitos puntos "sin medida".

Las matemáticas clásicas evitan introducir en sus razonamientos el "infinito actual", es decir, conjuntos formados por una infinidad de elementos simultáneamente existentes, conformándose con el "infinito potencial", que se

[1]Profesor de la Universidad de Halle. Publicó sus artículos básicos sobre Teoría de Conjuntos en "Mathematische Annalen" durante los años 1879-1893. Estos artículos fueron editados nuevamente en [C_2]; este volumen contiene también una biografía de Cantor escrita por Zermelo.

[2]Del griego $\pi\alpha\rho\grave{\alpha}\ \delta\grave{o}\xi\alpha$, expectación.

refiere a la posibilidad de aumentar toda magnitud dada. Si bien este punto de vista implicaba una cierta dosis de hipocresía, permitía al menos desarrollar la mayor parte de las matemáticas clásicas, incluyendo la teoría de las proporciones y más tarde el Cálculo Infinitesimal.

Las necesidades del Análisis (en particular el estudio a fondo de las funciones de variables reales que se desarrolla sobre todo durante el siglo XIX) son el origen de lo que iba a convertirse en la moderna Teoría de Conjuntos. Cuando Bolzano, en 1817, demuestra la existencia del extremo inferior de un conjunto de números reales acotado inferiormente, todavía razona, como la mayoría de sus contemporáneos, "en comprensión"; no hablando de un conjunto cualquiera de números reales, sino de una propiedad arbitraria de estos últimos. Pero cuando treinta años más tarde redacta sus *Paradoxien des - Unendlichen* (Paradojas del Infinito), no dudaba en reivindicar el derecho a la existencia del "infinito actual" y en hablar de conjuntos arbitrarios. En este trabajo define la noción general de equipotencia de conjuntos, y demuestra que cualesquiera dos intervalos compactos en $\mathbf{R}$ son equipotentes; observa también que la diferencia fundamental entre conjuntos finitos e infinitos radica en que un conjunto infinito E es equipotente a un subconjunto distinto de E, pero no da ninguna demostración convincente de esta afirmación. Por otra parte, el tono general de esta obra tiene mucho más de filosófico que de matemático, y no pudiendo separar de una forma suficientemente clara la noción de potencia o cardinalidad de un conjunto de la de magnitud y de la de orden de infinitud, fracasa en sus tentativas de formar conjuntos infinitos de potencias cada vez mayores y termina por intercalar en sus razonamientos una serie de consideraciones sobre las series divergentes, totalmente fuera de contexto.

La Teoría de Conjuntos, en el sentido que le damos hoy en día, se debe al genio de Georg Cantor. También él parte del Análisis y, sus estudios sobre las series trigonométricas, inspirados en los trabajos de Riemann (1826-1866), le llevan de modo natural, en 1872, a un primer intento de clasificación de los conjuntos "excepcionales" que aparecen en dicha teoría, mediante la noción de "conjuntos derivados sucesivos" que introduce con este fin. Como consecuencia de estas investigaciones y de su método para definir los números reales, Cantor comienza a interesarse por los problemas de equipotencia, ya que en 1873 hace notar que el conjunto de los números racionales (o el de los números algebraicos) es numerable. En su correspondencia con Dedekind, que da comienzo hacia esta fecha, le vemos plantear el problema de equipotencia entre el conjunto de los números enteros y el conjunto de todos los números reales, que resuelve algunas semanas más tarde. En 1874, Cantor intuye equivocadamente la imposibilidad de una biyección entre $\mathbf{R}$ y $\mathbf{R}^n$ $(n > 1)$. Posteriormente des-

cubre estupefacto que tal correspondencia biunívoca existe.

Una vez en posesión de estos resultados, tan nuevos como sorprendentes, se consagra por entero a la teoría de conjuntos. En una serie de seis memorias publicadas en los Mathematische Annalen entre 1878 y 1884 ataca simultáneamente los problemas de equipotencia, la teoría de conjuntos totalmente ordenados, las propiedades topológicas de $\mathbf{R}$ y $\mathbf{R}^n$, y el problema de la medida. Entre sus manos van deslindándose poco a poco, con una claridad admirable, nociones en apariencia indisolublemente unidas en la concepción clásica del "continuo". Ya en 1880 tiene la idea de iterar "transfinitamente" la formación de "conjuntos derivados", idea genitiva, que fructifica dos años después con la introducción de conjuntos bien ordenados, uno de los descubrimientos más originales de Cantor, que le permite abordar un estudio detallado de los números cardinales y formular el "problema del continuo".

Resultaba totalmente imposible que concepciones tan atrevidas, contrapuestas a una tradición dos veces milenaria, que concluían resultados tan inesperados y de un aspecto tan paradójico, se aceptasen sin resistencia. De hecho, entre los matemáticos influyentes de ese entonces en Alemania, Weiestrass (1815-1897) fue el único en seguir con cierto interés los trabajos de Cantor (que había sido alumno suyo); pero Cantor se encontró con una actitud de oposición empecinada por parte de Schwarz, y sobre todo de Kronecker. La tensión constante engendrada por la oposición a sus ideas, así como los esfuerzos infructuosos realizados para demostrar la hipótesis del continuo, parecen ser las causas de los primeros síntomas de una enfermedad nerviosa cuyos efectos sobre su producción matemática pronto se hicieron notar.

Dedekind, guiado por sus trabajos en Aritmética y sobre todo por la teoría de ideales, llegó a considerar la noción de conjunto ordenado desde un punto de vista más general que Cantor. Mientras que este último se limita a los conjuntos totalmente ordenados, Dedekind ataca el caso general y realiza un estudio profundo de los conjuntos reticulados. Estos trabajos no tuvieron gran audiencia en su momento; sus resultados fueron analizados posteriormente por diversos autores dando lugar a numerosas publicaciones desde 1935. La importancia histórica de los trabajos de Dedekind reside en el hecho de haber constituido uno de los primeros ejemplos de construcción axiomática; sin embargo, las aplicaciones de esta teoría han sido escasas. En contraposición, los primeros resultados de Cantor sobre conjuntos numerables y de la potencia del continuo dieron lugar rápidamente a numerosas e importantes aplicaciones, incluso dentro de las cuestiones más clásicas del Análisis.

Así pues, hacia finales del siglo XIX, las concepciones esenciales de Cantor habían ganado la partida. En esta misma época, se completa la formalización

de las matemáticas y el método axiomático fue casi universalmente aceptado. Pero simultáneamente surgía una "crisis de fundamentos" de proporciones considerables que conmovió al mundo matemático durante más de treinta años, y que parecía desquebrajar, no sólo todas las adquisiciones recientes en aquel entonces, sino también las partes más clásicas de la matemática.

En 1899 Cantor observa en una carta a Dedekind que no puede hablarse del "conjunto de todos los conjuntos" sin llegar a una contradicción. En 1905 Russell encontró que la noción del "conjunto de todos los conjuntos que no son elementos de sí mismos" es también contradictoria.

Podría pensarse que tales antinomias aparecían únicamente en regiones periféricas de las matemáticas, caracterizadas por considerar conjuntos de una "magnitud" inaccesible a la intuición. Eran razonamientos tan alejados del uso común de los matemáticos, que a muchos de ellos les parecían simples juegos de palabras. No obstante, estas paradojas insistían en señalar la necesidad de una revisión de las bases de la Teoría de Conjuntos a fin de eliminarlas. Pero si bien había unanimidad en cuanto a la urgencia de esta revisión, enseguida surgieron divergencias en la forma y método de llevarla a cabo. Pese a esto se trató de dar a la Teoría de Conjuntos una base axiomática como se hizo en el caso de la geometría elemental, donde no hay que ocuparse de a qué "cosas" se llama "*conjuntos*" ni de qué significa $x \in y$, sino que enumeren las condiciones impuestas a esta última relación. Naturalmente esta axiomatización se trató de hacer de tal manera que se pudieran abarcar en todo lo posible los resultados de Cantor, teniendo cuidado de evitar la aparición de conjuntos paradójicos.

El primer ejemplo de este tipo de axiomatización fue dado por Zermelo en 1904. En ésta, la introducción de conjuntos "muy grandes" se evita mediante un "axioma de comprensión" que grosso modo plantea que para determinar un conjunto con una propiedad $\mathbf{P}(x)$ es necesario (y suficiente) que $\mathbf{P}(x)$ implique una relación de la forma $x \in A$ para algún conjunto ya existente A. Después aparecieron otras axiomatizaciones de la Teoría de Conjuntos. Citamos principalmente la de Von Neumann mucho más cercana, que la de Zermelo, a la concepción primitiva de Cantor. Cantor había ya propuesto en su correspondencia con Dedekind la distinción de dos tipos de entes para evitar los conjuntos paradójicos: las "multiplicidades" y los "conjuntos" propiamente dichos; caracterizándose los segundos por ser pensados como un objeto único. Esta idea fue precisada por Von Neumann distinguiendo dos tipos de objetos: los "conjuntos" y las "clases". En su sistema (casi totalmente formalizado) las clases a diferencia de los conjuntos, no poden ser colocadas a la izquierda del signo $\in$. Una de las ventajas de este sistema es que rehabilita la noción de "clase

universal" empleada por los lógicos del siglo XIX (y que, naturalmente no es un conjunto). Además, la introducción de esquemas de axiomas es sustituida por axiomas convenientes, lo que simplifica el estudio lógico. Bernays y Gödel dieron variantes al sistema de Von Neumann.

La axiomatización de la teoría intuitiva de conjuntos de Cantor no sólo fue en sí misma un acontecimiento muy destacado en los avances de las matemáticas del siglo XX, también estableció que el método axiomático es posiblemente la manera más clara y precisa en la cual se puede dar una representación del conocimiento.

2

Axiomas de la Teoría de Conjuntos

2.1 Propiedades

Comúnmente los conjuntos son introducidos como colecciones de objetos con alguna propiedad común. La noción de propiedad merece un poco de análisis. Algunas propiedades frecuentemente consideradas en la vida diaria son tan vagas que difícilmente son admitidas en las matemáticas. Consideremos, por ejemplo, el "conjunto de todos los borregos gordos"; cabe preguntar ¿qué tan *gordo* es gordo? Si nos muestran algún borrego ¿cómo podemos saber si es gordo o no?

Como otro ejemplo, consideremos el "conjunto" de aquellos números naturales que pueden ser escritos (digamos que con papel y lápiz) en notación decimal. Claramente 0 puede ser escrito. Si un número n puede ser escrito, entonces seguramente el número $n+1$ también puede ser escrito. Por el familiar principio de inducción, cualquier número n puede ser escrito. Pero, ¿conoce o conocerá usted de alguien que pueda escribir el número $10^{10^{10}}$? Este número en notación decimal requiere de un 1 y 10^{10} ceros, que para lograr escribirse requiere de al menos trescientos años de trabajo continuo anotando un cero por segundo.

El problema para admitir a estas propiedades como "buenas" propiedades para definir conjuntos es causado por el significado vago de "puede". Una forma de remediar este tipo de dificultades o algunas otras similares es decir explícitamente qué significa "puede" o ponernos de acuerdo en qué significa "gordo"; por ejemplo, estableciendo que gordo es pesar más de cien kilogramos. Sin embargo, el determinar los elementos de un conjunto sabiendo que son los que satisfacen cierta propiedad, sigue siendo complicado. Para ilustrar esta afirmación, construiremos un "conjunto" en el que será más difícil ponerse de acuerdo en un criterio que permita definir bien el conjunto.

> Se cuenta que en un lejano poblado de un antiguo emirato había un barbero llamado As-Samet, *ducho en afeitar cabezas y barbas, maestro en escamondar sanguijuelas.* Un día el Emir, dándose cuenta de la escasez de barberos en el emirato, dio órdenes de que

> todos los barberos del emirato sólo afeitaran a aquellas personas que no pudieran hacerlo por sí mismas (todas las personas en este pueblo tienen que ser afeitadas, ya sea por el barbero o por ellas mismas). Un cierto día el barbero fue llamado a afeitar al Emir y le contó a éste sus congojas.
>
> — En mi pueblo soy el único barbero. Si me afeito, entonces puedo afeitarme por mí mismo y por lo tanto, no debería afeitarme el barbero de mi pueblo ¡que soy yo! Pero si no me afeito, lo debe hacer un barbero por mí ¡pero no hay allí más barbero que yo!
>
> El Emir pensó que tales razonamientos eran muy profundos, a tal grado que premió al barbero con la mano de la más virtuosa de sus hijas, y el barbero vivió eternamente feliz.

Consideremos como $\mathbf{P}(x)$ la propiedad "el habitante x del pueblo no se afeita a sí mismo (y, por tanto, es afeitado por el barbero)". Sea b el barbero. La cuestión es: ¿b tiene o no la propiedad?, es decir, ¿$\mathbf{P}(b)$ se verifica o no? Si b tiene la propiedad, entonces b no se afeita a sí mismo y es afeitado por el barbero. Pero b es el barbero, así que se afeita a sí mismo. Esto significa que b no tiene la propiedad. Si b no tiene la propiedad, entonces b se afeita a sí mismo y por lo tanto, no es afeitado por el barbero. Como b es el barbero, entonces b no se afeita a sí mismo, así que tiene la propiedad. En conclusión, no sabemos si b tiene o no la propiedad, pues la propiedad $\mathbf{P}(b)$ es cierta y falsa a la vez, es una paradoja, frecuentemente conocida como la paradoja del barbero.

Las propiedades anteriores y otras similares no definen conjuntos; esto es, todos los objetos que gozan de la propiedad no pueden ser coleccionados en un conjunto. Esta observación nos puede llevar a preguntar ¿qué propiedades sí definen conjuntos?. Desafortunadamente, no hay manera de conocer esto, y algunos resultados de lógica, especialmente el llamado Teorema de Incompletitud de Gödel, indican que una respuesta plena es imposible.

Para nosotros, *una propiedad es una proposición tal que para cualquier objeto es posible decidir, sin ambigüedad, si dicho objeto la verifica.* Si un objeto x verifica la propiedad $\mathbf{P}(x)$ decimos que la propiedad es verdadera (V); en caso contrario decimos que la propiedad es falsa (F). Cuando $\mathbf{P}(x)$ es verdadera también decimos que el objeto x tiene la propiedad $\mathbf{P}(x)$.

Desde propiedades arbitrarias $\mathbf{P}(x)$ y $\mathbf{Q}(x)$, podemos formar nuevas propiedades: la conjunción $\mathbf{P}(x) \wedge \mathbf{Q}(x)$, la disyunción $\mathbf{P}(x) \vee \mathbf{Q}(x)$ y la negación de $\mathbf{P}(x)$, $\neg\mathbf{P}(x)$. En cuanto al significado de estas nuevas propiedades generadas por $\mathbf{P}(x)$ y $\mathbf{Q}(x)$ tenemos que: Para que un objeto x verifique la conjunción es necesario que x verifique simultáneamente a cada una de las propiedades que

la componen; para que x verifique la disyunción es necesario que x verifique por lo menos una de sus componentes, y para que x verifique la negación de $\mathbf{P}(x)$ es necesario que x no verifique $\mathbf{P}(x)$. Los valores de verdad de estas propiedades pueden ser resumidos por la Tabla 1.

Tabla 1

$P(x)$	$Q(x)$	$P(x) \wedge Q(x)$	$P(x) \vee Q(x)$	$\neg P(x)$
V	V	V	V	F
V	F	F	V	F
F	V	F	V	V
F	F	F	F	V

La propiedad $\neg\left(\mathbf{P}(x) \wedge \neg\mathbf{Q}(x)\right)$ se abrevia como $\mathbf{P}(x) \Rightarrow \mathbf{Q}(x)$. La propiedad $[\mathbf{P}(x) \Rightarrow \mathbf{Q}(x)] \wedge [\mathbf{Q}(x) \Rightarrow \mathbf{P}(x)]$ se abrevia como $\mathbf{P}(x) \Leftrightarrow \mathbf{Q}(x)$. En la Tabla 2 se exponen los valores de verdad de estas propiedades en términos de los valores de verdad de sus componentes.

Tabla 2

$P(x)$	$Q(x)$	$P(x) \Rightarrow Q(x)$	$P(x) \Leftrightarrow Q(x)$
V	V	V	V
V	F	F	F
F	V	V	F
F	F	V	V

Una cuantificación existencial es una propiedad de la forma $\exists x\, \mathbf{P}(x)$, donde $\mathbf{P}(x)$ es una propiedad cualquiera conocida como cuantificado y $\exists$ es el cuantificador existencial. La propiedad $\exists x\, \mathbf{P}(x)$ es verdadera si $\mathbf{P}(x)$ es verdadera para al menos un objeto x; de otro modo es falsa. La propiedad $\forall x\, \mathbf{P}(x)$, conocida como cuantificación universal, es una abreviación de la propiedad $\neg(\exists x)\,(\neg\mathbf{P}(x))$.

Abreviaremos con $\forall x \in X,\, \mathbf{P}(x)$ la propiedad $\forall x\,(x \in X \Rightarrow \mathbf{P}(x))$ y denotaremos por $\exists x \in X,\, \mathbf{P}(x)$ a la propiedad $\exists x\,(x \in X \wedge \mathbf{P}(x))$.

Una propiedad puede depender de más de un parámetro. Una propiedad del estilo $\mathbf{P}(x, y, \ldots z)$ tiene varios parámetros (una cantidad finita), y su valor de verdad depende de todos los parámetros.

2.2 Los Axiomas

Como se aseguró en la introducción, el enfoque adoptado para el desarrollo de la Teoría de Conjuntos será axiomático y la manera de realizar esta axiomática

será parecida a aquella de la Geometría. Es decir, en nuestra axiomática no examinaremos directamente el significado del término "*conjunto*" —tal y como en Geometría no se examinan los significados de los términos "punto", "recta" y "plano"—; pero a partir de sus axiomas —al igual que en Geometría— se deducen todos los teoremas sin recurrir a los significados intuitivos de los términos primitivos.

Los axiomas tienen su origen en el concepto intuitivo de conjunto, pero el método axiomático asegura que el concepto intuitivo de la palabra "conjunto" no interviene en las demostraciones de teoremas o en definiciones de conceptos conjuntistas.

Las nociones primitivas de la Teoría de Conjuntos son "conjunto", y la relación de pertenencia "ser un elemento de", la cual se simbolizará por $\in$; su negación: x no es un elemento o miembro de y la denotamos con $x \notin y$.[1] Para simplificar la notación usaremos letras mayúsculas para referirnos a conjuntos. En ocasiones (cuando sea posible) indicaremos la jerarquía de un conjunto denotándolo con letras caligráficas.

Ahora empezaremos a dar nuestro sistema axiomático. Intentaremos aclarar el significado intuitivo de cada axioma.

Para dar sustancia a la discusión, el primer axioma que adoptaremos postula que al menos existe un conjunto. Para concretar, postularemos la existencia de un conjunto específico, a saber, el conjunto vacío. Ya que más adelante formularemos una suposición de existencia más profunda y más útil, la siguiente juega sólo un papel temporal.

Axioma 1 (de Existencia) *Hay un conjunto que no tiene elementos.*

Un conjunto sin elementos puede ser descrito de manera intuitiva de varias formas; por ejemplo, como "el conjunto de los perros que han escrito obras literarias" o como "el conjunto de números reales que satisfacen la ecuación $x^2 + 1 = 0$". Intuitivamente los ejemplos de esta clase describen al mismo conjunto, a saber, el conjunto vacío, conjunto vacuo. Pero no podemos probar esta afirmación; necesitamos otro axioma que exprese el hecho de que un conjunto está determinado por sus elementos, tal y como intuitivamente lo concebimos.

Axioma 2 (de Extensión) *Si todo elemento de X es un elemento de Y, y todo elemento de Y es un elemento de X, entonces $X = Y$.*

---

[1] El símbolo $\in$ se deriva de la letra griega épsilon. El uso de esta letra para la relación de pertenencia fue introducido por Peano [P_2] quien la seleccionó como abreviación de la palabra Griega estar ($\grave{\varepsilon}\sigma\tau\acute{\iota}$)

El Axioma de Extensión puede expresarse en otras palabras diciendo: dos conjuntos que tienen los mismos elementos son idénticos. Simbólicamente este axioma puede expresarse así:

$$X = Y \quad \Leftrightarrow \quad (\forall x : x \in X \ \Rightarrow \ x \in Y) \ \wedge \ (\forall x : x \in Y \ \Rightarrow \ x \in X).$$

Por otra parte, es valioso comprender que el *Axioma de Extensión no es sólo una propiedad lógicamente necesaria de la igualdad, sino que es una proposición no trivial acerca de la pertenencia*. Una manera de llegar a entender este punto es considerar una situación en la cual el análogo al Axioma de Extensión no se cumpla. Supóngase, por ejemplo, que consideramos seres humanos como (en lugar de) conjuntos y que, si x y A son seres humanos, escribiremos $x \in A$ siempre que x es un ancestro de A (por ejemplo, $x \in A$ si x es padre de A o si x es bisabuelo de A). El análogo del Axioma de Extensión diría en este caso que "dos seres humanos tienen los mismos ancestros si y sólo si son iguales". Pero, ¿qué pasa con dos hermanos?

Proposición 2.1 *Hay un único conjunto que no tiene elementos.*

Demostración:

Asumamos que A y B no tienen elementos. Entonces todo elemento de A es un elemento de B (puesto que A no tiene elementos la proposición "$a \in A \ \Rightarrow \ a \in B$" es automáticamente cierta). Similarmente, todo elemento de B es un elemento de A. Por el Axioma de Extensión concluimos que $A = B$. ■

La proposición anterior nos posibilita para hacer la siguiente definición.

Definición 2.2 El único conjunto que no tiene elementos es llamado el *conjunto vacío* y es denotado por $\emptyset$.

Intuitivamente, los conjuntos son colecciones de objetos que satisfacen alguna propiedad, y sería deseable tener un axioma que exprese este hecho. Este axioma retomaría el espíritu de la "definición" de conjunto dada por Cantor. El problema es que no toda propiedad describe un conjunto, pues algunas propiedades pueden introducir paradojas y nuestra intención al axiomatizar la Teoría de Conjuntos es precisamente evitar las paradojas. En seguida demostraremos que la colección $\{x : x \text{ es un conjunto}\}$ no es un conjunto, es decir, la propiedad $\mathbf{P}(x)$: "x es un conjunto", no describe en realidad un conjunto.

El problema estará resuelto si postulamos solamente la existencia del conjunto de todos los objetos que tienen una propiedad dada, los cuales pertenezcan a otro conjunto ya dado de antemano. El siguiente axioma puede considerarse como de los más importantes, pues permite la construcción de nuevos conjuntos a partir de otros ya existentes.

Axioma 3 (Esquema de Comprensión) *Sea* $\mathbf{P}(x)$ *una propiedad de* x*. Para cualquier conjunto* A *hay un conjunto* B *tal que* $x \in B$ *si y sólo si* $x \in A$ *y* $\mathbf{P}(x)$.

En contraste a los otros axiomas, los cuales son proposiciones, el Axioma Esquema de Comprensión es una colección infinita de proposiciones. Esto es, éste es un esquema para producir axiomas, uno por cada elección de la propiedad $\mathbf{P}$. Por ejemplo, si $\mathbf{P}(x)$ es "$x = x$" el axioma dice: Para cualquier conjunto A, hay un conjunto B tal que $x \in B$ si y sólo si $x \in A$ y $x = x$. (En este caso $A = B$). Si $\mathbf{P}(x)$ es "$x \notin x$", el axioma postula: Para cualquier conjunto A hay un conjunto B tal que $x \in B$ si y sólo si $x \in A$ y $x \notin x$. Por lo anterior el Axioma 3 se llama *Esquema de Comprensión.*

La propiedad $\mathbf{P}(x)$ puede depender de otras variables $p, q, \ldots, r$; el correspondiente axioma postula entonces que para cualquier selección de las variables $p, q, \ldots, r$, y cualquier conjunto A, hay un conjunto B (que depende de $p, q, \ldots, r$ y A) que consiste exactamente de los elementos de A para los cuales se verifica $\mathbf{P}(x, p, q, \ldots, r)$.

Ejemplo 2.3 Si P y Q son conjuntos, entonces hay un conjunto R tal que $x \in R$ si y sólo si $x \in P$ y $x \in Q$.

Demostración:

Considérese la propiedad $\mathbf{P}(x, Q)$ de x y Q: "$x \in Q$". Entonces por el Axioma Esquema de Comprensión, para todo Q y cualquier P hay un conjunto R tal que $x \in R$ si y sólo si $x \in P$ y $\mathbf{P}(x, Q)$, es decir, si y sólo si $x \in P$ y $x \in Q$. ■

Ejemplo 2.4 El conjunto de todos los conjuntos no existe.

Demostración:

Supongamos lo contrario, sea $\mathcal{U}$ el conjunto de todos los conjuntos y consideremos la propiedad $\mathbf{P}(x)$: "$x \notin x$". El Axioma 3 nos dice que existe un conjunto R tal que $x \in R$ si y sólo si $x \in \mathcal{U}$ y $x \notin x$; o sea, x es un elemento de R si y sólo si x es un conjunto y x no es miembro de sí mismo. Como R es un conjunto entonces $R \in \mathcal{U}$, así entonces R puede o no verificar la propiedad $\mathbf{P}$. Si $R \notin R$ entonces $R \in R$, es decir, $(R \notin R) \wedge (R \in R)$, una contradicción.

Por otro lado, si $R \in R$ entonces R sí verifica la propiedad $\mathbf{P}$, es decir, $R \notin R$, nuevamente $(R \in R) \wedge (R \notin R)$, una contradicción. Por lo tanto, suponer la existencia de $\mathcal{U}$ y considerar la propiedad legítima $\mathbf{P}$ siempre lleva a una contradicción, concluimos que no existe tal conjunto $\mathcal{U}$. ■

Nótese que de hecho $\mathcal{U}$ mismo no es esencial para el razonamiento anterior. En efecto, si en lugar de $\mathcal{U}$ tomáramos otro conjunto cualquiera X y razonamos por medio del Axioma Esquema de Comprensión de la misma manera que en la demostración anterior, tendríamos que concluir que $R \notin X$. Esta deducción es interesante, pues nos permite decir que hay algo (es decir, R) que no pertenece a X. Como el conjunto X en este razonamiento es arbitrario, hemos demostrado que *no hay un conjunto que contenga todo*, o bien que *no hay un universo*. "Universo" se usa aquí en el sentido de "universo de discurso", lo cual significa, en cualquier discusión particular, un conjunto que contiene a todos los objetos que intervienen en ese estudio. En tratamientos más antiguos (preaxiomáticos) a la Teoría de Conjuntos, se daba por supuesta la existencia de un universo.

El razonamiento del Ejemplo 2.4 se conoce como *la Paradoja de Russell*[2] y en la literatura toma muchas formas equivalentes a la que hemos planteado aquí. La moraleja es que es imposible, especialmente en matemáticas, obtener algo a partir de nada. *Para especificar un conjunto no basta dar una propiedad; es necesario también disponer de un conjunto a cuyos elementos pueda aplicarse esa propiedad.* Esta es la limitación impuesta por el Axioma 3; la manera de suprimir las dificultades que surgen al definir "conjuntos muy grandes" es proceder a la inversa, garantizando por medio de axiomas la existencia de conjuntos mínimos y la obtención de nuevos conjuntos a partir de los ya existentes.

En capítulos posteriores tendremos la oportunidad de conocer otras colecciones (distintas de $\mathcal{U}$, la colección de todos los conjuntos) que no son conjuntos; pero nos permitimos hacer la siguiente:

Convención 2.5 Si $\mathbf{P}(x)$ es una propiedad de x, a

$$\mathbf{K} = \langle x : x \text{ es un conjunto y } \mathbf{P}(x) \rangle$$

le llamaremos clase.

Debe quedar claro que no se está definiendo lo que es una clase, la convención anterior nos facilitará más adelante referirnos a ciertas colecciones. La

[2]En 1903 fue publicada por primera vez la Paradoja de Russell, en el apéndice de [F$_4$].

discusión anterior también nos dice que una clase *no necesariamente* es un conjunto. La diferencia entre estos dos conceptos originó parte de los problemas lógicos de Cantor.

Lema 2.6 *Sea* $\mathbf{P}(x)$ *una propiedad de* x*. Para todo* A *hay un único conjunto* B *tal que* $x \in B$ *si y sólo si* $x \in A$ *y* $\mathbf{P}(x)$*.*

Demostración:

Si B' es un conjunto tal que $x \in B'$ si y sólo si $x \in A$ y $\mathbf{P}(x)$, entonces $x \in B$ si y sólo si $x \in B'$. Así, $B = B'$ por el Axioma de Extensión. ■

Ahora tenemos derecho de hacer la siguiente definición que provee de una notación al conjunto B unívocamente determinado.

Definición 2.7 $\{x \in A : \mathbf{P}(x)\}$ es el conjunto de todos los $x \in A$ con la propiedad $\mathbf{P}(x)$.

Nuestro sistema axiomático hasta este momento no es muy poderoso; el único conjunto cuya existencia postulamos es el conjunto vacío, y las aplicaciones del Esquema de Comprensión a éste, producen nuevamente el conjunto vacío: para cualquier propiedad $\mathbf{P}(x)$, $\{x \in \emptyset : \mathbf{P}(x)\} = \emptyset$. Los siguientes tres axiomas postulan que algunos de los procedimientos frecuentemente usados en matemáticas producen conjuntos.

Axioma 4 (del Par) *Para cualesquiera* a *y* b *hay un conjunto* C *tal que* $x \in C$ *si y sólo si* $x = a$ *o* $x = b$*.*

Así, $a \in C$ y $b \in C$, y no hay otros elementos en C. Por el Axioma de Extensión el conjunto C es único. Definimos el *par no ordenado* de a y b como el conjunto que tiene a a y a b como elementos, y lo denotamos por $\{a, b\}$. Podemos formar el par no ordenado $\{a, a\}$ el cual se denota simplemente por $\{a\}$, y se llama conjunto *singular* o *unitario* de a.

El Axioma del Par asegura que todo conjunto es un elemento de algún conjunto, y dos conjuntos cualesquiera son simultáneamente elementos de algún mismo conjunto.

Ejemplo 2.8 Sean $A = \emptyset$ y $B = \emptyset$, entonces $\{\emptyset\} = \{\emptyset, \emptyset\}$ es un conjunto tal que $\emptyset \in \{\emptyset\}$. Note que $\emptyset \neq \{\emptyset\}$, puesto que $\emptyset$ no tiene elementos y $\{\emptyset\}$ tiene un elemento.

Ejemplo 2.9 Sean $A = \emptyset$ *y* $B = \{\emptyset\}$. Entonces $\emptyset \in \{\emptyset, \{\emptyset\}\}$ *y* $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$*;* además, $\emptyset$ *y* $\{\emptyset\}$ son los únicos elementos de $\{\emptyset, \{\emptyset\}\}$. Note que $\emptyset \neq \{\emptyset, \{\emptyset\}\}$ y $\{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$.

Ejemplo 2.10 Sean $A = \{\emptyset\}$ y $B = \{\emptyset\}$, entonces $\emptyset \in \{\emptyset\}$ y $\{\emptyset\} \in \{\{\emptyset\}\}$. Pero $\emptyset \notin \{\{\emptyset\}\}$, ya que el único elemento del conjunto $\{\{\emptyset\}\}$ es $\{\emptyset\}$, y por el Ejemplo 2.8, $\emptyset \neq \{\emptyset\}$.

Del ejemplo anterior podemos deducir que $\emptyset \neq \{\{\emptyset\}\}$ y que $\{\emptyset\} \neq \{\{\emptyset\}\}$, lo cual nos permite inferir la existencia de muchísimos conjuntos singulares como: $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, $\ldots, \{\cdots\{\{\emptyset\}\}\cdots\}$, o bien pares no ordenados como $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$, etc. Sin embargo, una pregunta interesante es: ¿Son realmente distintos estos conjuntos? La respuesta se deja como un ejercicio, aquí únicamente notaremos que no debemos confundir los conjuntos de un solo elemento con el elemento propiamente dicho. No es cierto que x y $\{x\}$ sean iguales, lo cual puede confirmarse observando que $\{x\}$ sólo tiene un miembro, a saber x; mientras que x puede tener cualquier número de miembros. Véase el Ejemplo 2.8 y más adelante el Teorema 2.33 para derivar razones más convincentes.

Si A y B son conjuntos, es deseable reunir a sus elementos en un solo conjunto. Este conjunto es diferente del que se construyó con el Axioma 4: mientras que los elementos del par no ordenado son los conjuntos A y B, nuestro nuevo conjunto tendrá por elementos a los elementos de A y B (ver Ejemplo 2.15).

Axioma 5 (de Unión) *Para cualquier conjunto S, existe un conjunto U tal que $x \in U$ si y sólo si $x \in X$ para algún $X \in S$.*

Nuevamente el conjunto U es único. Éste es llamado *unión* de S y denotado por $\bigcup S$. Decimos que S es un *sistema de conjuntos o familia de conjuntos* cuando queremos hacer énfasis en que los elementos de S son conjuntos. La unión de una familia de conjuntos S es entonces el conjunto de, precisamente, todos los x que pertenecen a algún conjunto que forma parte de la familia S.

Ejemplo 2.11 Sea $S = \{\emptyset, \{\emptyset\}\}$; entonces $x \in \bigcup S$ si y sólo si $x \in A$ para algún $A \in S$, *es decir*, si y sólo si $x \in \emptyset$ o $x \in \{\emptyset\}$. Por lo tanto, $x \in \bigcup S$ si y sólo si $x = \emptyset$; o sea, $\bigcup S = \{\emptyset\}$.

Ejemplo 2.12 $\bigcup \emptyset = \emptyset$

Ejemplo 2.13 Sean A y B conjuntos, $x \in \bigcup \{A, B\}$ si y sólo si $x \in A$ o $x \in B$. El conjunto $\bigcup \{A, B\}$ es llamado la unión de A *y* B y es denotado por $A \cup B$.

Obsérvese que el Axioma del Par y el Axioma de Unión son necesarios para definir la unión de dos conjuntos, y el Axioma de Extensión es necesario para

garantizar la unicidad. Además nótese que la unión de dos conjuntos tiene el significado usual:

$$x \in A \cup B \qquad \Leftrightarrow \qquad x \in A \quad \vee \quad x \in B.$$

Ejemplo 2.14 $\{\{\emptyset\}\} \cup \{\emptyset, \{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$

Ejemplo 2.15 Si $A = \{\emptyset, \{\emptyset\}\}$ y $B = \{\{\{\emptyset\}\}\}$, entonces el par no ordenado de A y B es distinto de $A \cup B$.

El Axioma de Unión es muy poderoso; éste nos capacita no sólo para formar uniones de dos conjuntos, sino también para formar la unión de un número infinito de conjuntos (más tarde se aclarará tal situación).[3]

Dados a, b y c, puede probarse la unicidad del conjunto P cuyos elementos son exactamente a, b y c, en efecto $P = \{a, b\} \cup \{c\}$. P es denotado por $\{a, b, c\}$ y se llama *terna no ordenada* de a, b y c. Análogamente puede definirse una cuarteta, quinteta, sexteta no ordenada, etc.

Ahora introduciremos un concepto simple y familiar para el lector.

Definición 2.16 A es un *subconjunto* de B si cualquier elemento de A pertenece a B. En otras palabras, A es un subconjunto de B si, para todo x, $x \in A$ implica $x \in B$. Escribiremos $A \subseteq B$ o $B \supseteq A$ para denotar que A es subconjunto de B.

Ejemplo 2.17 $\{\emptyset\} \subseteq \{\emptyset, \{\emptyset\}\}$ y $\{\{\emptyset\}\} \subseteq \{\emptyset, \{\emptyset\}\}$.

Ejemplo 2.18 $x \in A$ si y sólo si $\{x\} \subseteq A$.

Según la Definición 2.16, todo conjunto debe considerarse subconjunto de sí mismo.

Ejemplo 2.19 $\emptyset \subseteq A$ y $A \subseteq A$ para todo conjunto A.

Ejemplo 2.20 Para cualesquiera conjuntos A, B y C tales que $A \subseteq B$ y $B \subseteq C$ se tiene que $A \subseteq C$.

El Axioma Esquema de Comprensión puede ahora interpretarse como un axioma que nos permite la formación de subconjuntos.

Ejemplo 2.21 $\{x \in A : \mathbf{P}(x)\} \subseteq A$.

---

[3]Las nociones de finito e infinito serán formalizadas posteriormente, por el momento las emplearemos en forma intuitiva.

Ejemplo 2.22 Si $A \in S$ entonces $A \subseteq \bigcup S$.

Si A y B son dos conjuntos tales que $A \subseteq B$ y $B \subseteq A$, entonces A y B tienen los mismos elementos y, por lo tanto, en virtud del Axioma de Extensión, $A = B$. De hecho el Axioma de Extensión puede ser formulado en estos términos: Si A y B son dos conjuntos, una condición necesaria y suficiente para que $A = B$ es que $A \subseteq B$ y $B \subseteq A$ simultáneamente. Por lo anterior, casi todas las demostraciones de igualdad entre dos conjuntos A y B están divididas en dos partes, hacer ver primero que $A \subseteq B$ y mostrar después que $B \subseteq A$.

Obsérvese que la pertenencia ($\in$) y la contención ($\subseteq$)[4] son, conceptualmente, cosas muy diferentes. Una diferencia importante es la que manifiesta el Ejemplo 2.19 al mostrarnos que para cualquier conjunto A, $A \subseteq A$ mientras que no está del todo claro que cualquier conjunto A, $A \in A$. Indudablemente que esto último no es posible para cualquier conjunto razonable, de hecho $\emptyset \notin \emptyset$ y por ende $\subseteq$ es reflexiva pero $\in$ no lo es. Sin embargo, no podremos demostrar que para cualquier conjunto A, $A \notin A$, hasta que introduzcamos el Axioma de Fundación. Otra diferencia entre $\in$ y $\subseteq$ la podemos derivar de los Ejemplos 2.10 y 2.20 como sigue: $\emptyset \in \{\emptyset\}$ y $\{\emptyset\} \in \{\{\emptyset\}\}$ pero $\emptyset \notin \{\{\emptyset\}\}$, es decir, la pertenencia ($\in$) a diferencia de la contención ($\subseteq$) no tiene carácter transitivo.

Ahora introducimos el siguiente axioma, el cual nos asegura que dado un conjunto cualquiera podemos formar un nuevo conjunto cuyos miembros son exactamente los subconjuntos del conjunto dado; en forma precisa:

Axioma 6 (del Conjunto Potencia) *Para cualquier conjunto X existe un conjunto S tal que $A \in S$ si y sólo si $A \subseteq X$.*

Puesto que el conjunto S está unívocamente determinado, llamamos al conjunto S de todos los subconjuntos de X, el *conjunto potencia* de X y es denotado por $\mathcal{P}(X)$.

Ejemplo 2.23 $\mathcal{P}(\emptyset) = \{\emptyset\}$.

Ejemplo 2.24 $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$.

Ejemplo 2.25 $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Ejemplo 2.26 Para cualquier conjunto X, siempre $\emptyset, X \in \mathcal{P}(X)$. En particular siempre se cumple $\mathcal{P}(X) \neq \emptyset$ para cualquier X.

Ejemplo 2.27 Si $A \subseteq B$ entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

[4]El crédito de la distinción entre pertenencia y contención se da generalmente a Peano, quien introdujo diferentes notaciones para los dos conceptos.

Ejemplo 2.28 Si $X = \{\emptyset, a, b, \{a\}\}$ y $A = \{a\} \subseteq X$ entonces $\mathcal{P}(A) \subseteq X$.

Ejemplo 2.29 Si $X = \{\emptyset, a, b\}$ y $A = \{a\}$ entonces $\mathcal{P}(A) \nsubseteq X$.

A continuación responderemos la pregunta: ¿Para algún conjunto X puede ocurrir que $X \in X$? Para conjuntos "razonables" que a uno se le puedan ocurrir la respuesta es indudablemente no, pero en realidad esta pregunta no puede ser respondida sin el siguiente axioma.

Axioma 7 (de Fundación) *En cada conjunto no vacío A existe $u \in A$ tal que u y A no tienen elementos en común, es decir, para cualquier x, si $x \in A$ entonces $x \notin u$.*

Este axioma también se conoce como Axioma de Regularidad y postula que "conjuntos" de cierto tipo no existen. Esta restricción no es contradictoria (es decir, el axioma es consistente con los otros axiomas) y es irrelevante para el desarrollo de los números naturales, reales, cardinales u ordinales; y de hecho para casi todas las matemáticas ordinarias. Sin embargo, es extremadamente útil en las matemáticas de la Teoría de Conjuntos, para la Construcción de Modelos.[5] En [A_1] se desarrolla una Teoría de Conjuntos con la negación del Axioma de Fundación.

Ejemplo 2.30 Si $A = \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ entonces $u = \{\emptyset\}$ y A no tienen elementos en común.

Ejemplo 2.31 Si $A = \{\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$ entonces $\{\{\{\emptyset\}\}\}$ y A tienen a $\{\{\emptyset\}\}$ como elemento común. También $\{\{\emptyset\}\}$ y A tienen a $\{\emptyset\}$ como elemento común, pero $\{\emptyset\}$ y A no tienen elementos comunes.

Ejemplo 2.32 Si $\emptyset \in A$ entonces tomando a $u = \emptyset$ tenemos que u y A no tienen elementos comunes.

Teorema 2.33 *(a) Ningún conjunto no vacío puede ser elemento de sí mismo, es decir, para cualquier $X \neq \emptyset$, $X \notin X$.*

(b) Si A y B son conjuntos no vacíos, entonces no es posible que ocurran simultáneamente $A \in B$ y $B \in A$.

---

[5] En 1994 H. Andréka, I. Németi y Á. Kurucz demostraron que el Axioma de Fundación es necesario para derivar un importante teorema del Álgebra Universal como es el Teorema de Variedad de Birkhoff. [AKN]

DEMOSTRACIÓN:

(a) Supongamos que existe un conjunto no vacío X tal que $X \in X$. Por el Axioma del Par, $\{X\}$ también es un conjunto, y puesto que X es el único miembro de $\{X\}$, el conjunto $\{X\}$ contradice el Axioma de Fundación, ya que X y $\{X\}$ tienen a X como elemento común, es decir, todo elemento de $\{X\}$ tiene un elemento común con $\{X\}$.

(b) Para este caso considere el par no ordenado $\{A, B\}$ y proceda de modo análogo a *(a)*. ■

La parte *(a)* del teorema anterior responde a la pregunta planteada anteriormente: ¿para algún conjunto X puede ocurrir que $X \in X$? Mientras que de la parte *(b)* podemos deducir que no pueden existir ciclos de la forma $A \in B \in A$.

Hasta ahora nuestra lista de axiomas no está completa. Pospondremos los restantes para capítulos ulteriores cuando introduzcamos otros conceptos y hayamos establecido algunos teoremas que nos permitirán entenderlos.

Ahora introduciremos una notación convencional. Sea $\mathbf{P}(x)$ una propiedad de x (y, posiblemente de otros parámetros). Si hay un conjunto A tal que para todo x, $\mathbf{P}(x)$ implica $x \in A$, entonces $\{x \in A : \mathbf{P}(x)\}$ existe; y más aún, no depende de quién sea el conjunto A. En efecto, si A' es otro conjunto tal que, para todo x, $\mathbf{P}(x)$ implica $x \in A'$, entonces

$$\{x \in A' : \mathbf{P}(x)\} = \{x \in A : \mathbf{P}(x)\}.$$

Podemos ahora definir $\{x : \mathbf{P}(x)\}$ como el conjunto $\{x \in A : \mathbf{P}(x)\}$, donde A es cualquier conjunto para el que $\mathbf{P}(x)$ implica $x \in A$. $\{x : \mathbf{P}(x)\}$ es el conjunto de todo x que tiene la propiedad $\mathbf{P}(x)$. Enfatizamos nuevamente que esta notación podrá ser usada solamente después que se haya probado que algún conjunto A contiene a todos los x con la propiedad $\mathbf{P}(x)$. Recuerde que lo que llamamos clase tiene otra notación, a saber, $\langle x : \mathbf{P}(x) \rangle$.

Ejemplo 2.34 $\{x : (x \in P) \wedge (x \in Q)\}$ existe.

DEMOSTRACIÓN:

Sea $\mathbf{P}(x, P, Q)$ la propiedad "$x \in P$ y $x \in Q$". Sea $A = P$; entonces $\mathbf{P}(x, P, Q)$ implica $x \in A$. Por lo tanto,

$$\{x : (x \in P) \wedge (x \in Q)\} = \{x \in P : (x \in P) \wedge (x \in Q)\} = \{x \in P : x \in Q\}$$

es el conjunto del Ejemplo 2.3. ■

Ejemplo 2.35 $\{x : (x = a) \vee (x = b)\}$ existe. Para una prueba, tómese $A = \{a, b\}$ y demuéstrese que $A = \{x : (x = a) \vee (x = b)\}$.

Ejemplo 2.36 $\{x : x \notin x\}$ no existe (recuérdese la *Paradoja de Russell* Ejemplo 2.4); así en este caso, la notación $\{x : \mathbf{P}(x)\}$ es inadmisible.

Como ya se dijo, la primera axiomatización de la Teoría de Conjuntos fue dada por Zermelo [Z_2]. La formulación del Axioma Esquema de Comprensión, al cual le llamaba *Aussonderungsaxiom*, fue más bien ambiguo y dio lugar a serias discusiones; la versión adoptada fue formulada por T. Skolem [S_7] en 1922. El Axioma de Fundación fue propuesto por D. Mirimanoff en 1917.

Russell y Whitehead en su famoso *Principia Mathematica* (primera edición 1910-1913) dieron también una de las primeras y más influyentes axiomatizaciones para la Teoría de Conjuntos. Ellos evitaban las paradojas introduciendo la llamada "teoría de tipos"; en la cual se definen una cantidad infinita de diferentes tipos de variables de conjuntos. Para cada tipo de variables de conjuntos hay una cantidad infinita de variables del siguiente tipo superior. La propiedad "x es un miembro de y" tiene significado si y sólo si y es de exactamente un tipo superior a x. La paradoja de Russell, por ejemplo, al estar representada por la propiedad "x no es un miembro de x" carece de sentido en la teoría de tipos. Ya que la teoría de tipos es complicada, y puesto que es pesado dar seguimiento a todos los tipos de variables, esta teoría es inconveniente para el desarrollo de las matemáticas.

Otra axiomatización de la Teoría de Conjuntos fue propuesta por Quine en 1931. Su enfoque puede decirse que es mas bien semántico; él dio reglas para la construcción de propiedades. La teoría de Quine es más manejable que la teoría de los tipos pero contiene fallas fatales que no permite desarrollar la matemática a partir de esta teoría. Specker [S_8] en 1953 demostró que el Axioma de Elección (que después formularemos) es inconsistente en el sistema de Quine.

Von Neumann [N_2], [N_3] entre 1925 y 1928 propuso otra axiomatización en la cual se hacía preciso el ambiguo Axioma Esquema de Comprensión de Zermelo. En lugar de usar propiedades como Skolem, Von Neumann admitió una nueva noción primitiva dentro de la Teoría de Conjuntos: la de *clase*. Este sistema fue posteriormente reformulado por Bernays [B_1] en 1937 y por Gödel [G_2] en 1938. La ventaja del sistema resultante, llamado en la literatura "sistema **BG**", es que está basado en un número finito de axiomas. Otros sistemas axiomáticos fueron propuestos por Morse y por Kelley [M_5], [K_3].

Ejercicios 2.2

1. Muestre que los conjuntos $\emptyset$, $\{\emptyset\}$, $\{\{\emptyset\}\}$, $\ldots$, $\{\cdots\{\emptyset\}\cdots\}$ son distintos.
2. Indique cuáles de las siguientes expresiones son falsas:

$$\text{(a) } A = \{A\}, \qquad \text{(b) } \{a,b\} = \{\{a\},\{b\}\}, \qquad \text{(c) } \emptyset \in \{\emptyset\}.$$

3. Muestre que el conjunto de todos los x tales que $x \in A$ y $x \notin B$ existe. ¿Es único?
4. Pruebe que para cualquier conjunto X hay algún $a \notin X$.
5. Demuestre la unicidad del conjunto U asegurado por el Axioma de Unión.
6. Pruebe que $\bigcup \emptyset = \emptyset$.
7. Verifique la afirmación hecha en el Ejemplo 2.15.
8. Sean A y B conjuntos. Muestre que existe un único conjunto C tal que $x \in C$ si y sólo si ($x \in A$ y $x \notin B$) o ($x \in B$ y $x \notin A$).
9. Demuestre que $\{a\} = \{b,c\}$ si y sólo si $a = b = c$.
10. (a) Muestre que para cualesquiera conjuntos A, B y C existe un único conjunto P tal que $x \in P$ si y sólo si $x = A$ o $x = B$ o $x = C$.
    (b) Generalice (a) para cuatro o más elementos.
11. Demuestre que $A \subseteq \{A\}$ si y sólo si $A = \emptyset$.
12. Verifique las afirmaciones de los Ejemplos 2.18, 2.19, 2.20.
13. Pruebe la afirmación del Ejemplo 2.22.
14. Demuestre que si $A \subseteq B$ entonces $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
15. Pruebe la afirmación del Ejemplo 2.35.
16. Complete la demostración del Teorema 2.33(b).
17. Pruebe que es imposible la existencia de un ciclo:

$$A_0 \in A_1 \in A_2 \in \cdots \in A_n \in A_0$$

para toda $n \in \mathbf{N}$.

18. (a) Demuestre que para cualquier conjunto X es falso que $\mathcal{P}(X) \subseteq X$. En particular $X \neq \mathcal{P}(X)$.

    (b) Demuestre que el conjunto de todos los conjuntos no existe usando el inciso (a).

19. Reemplace el Axioma de Existencia por el siguiente axioma:
    Axioma Débil de Existencia. Existe al menos un conjunto.
    Deduzca el Axioma de Existencia usando el Axioma Débil de Existencia y el Axioma Esquema de Comprensión.

20. El Axioma de Unión, el Axioma del Par y el Axioma del Conjunto Potencia pueden reemplazarse por las siguientes versiones más débiles:
    Axioma Débil del Par. Para cualesquiera a, b existe un conjunto C tal que $a \in C$ y $b \in C$.
    Axioma Débil de Unión. Para cualquier conjunto S existe un conjunto U tal que si $x \in A$ y $A \in S$ entonces $x \in U$.
    Axioma Débil del Conjunto Potencia. Para cualquier conjunto S existe un conjunto P tal que $X \subseteq S$ implica $X \in P$.
    Deduzca el Axioma del Par, el Axioma de Unión y el Axioma del Conjunto Potencia, usando las versiones débiles. (Sugerencia: use el Axioma Esquema de Comprensión).

3

Álgebra de Conjuntos

En este capítulo, como en los siguientes, estudiaremos las operaciones conjuntistas más comunes, por lo que momentáneamente supondremos la existencia de conjuntos como el de los números naturales $\mathbf{N}$,[1] el de los números reales $\mathbf{R}$, o conjuntos que de ellos se desprenden; esto es sólo con el afán de proporcionar ejemplos ilustrativos de los conceptos que tratemos. La existencia de estos conjuntos será formalizada en su momento.

3.1 Operaciones Fundamentales

En el capítulo anterior la Definición 2.16 reza "A se dice subconjunto de B, $A \subseteq B$, si todo elemento de A es también un elemento de B". La relación de contención $\subseteq$ tiene las siguientes propiedades para conjuntos A, B y C.

(1) $A \subseteq A$.
(2) Si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.
(3) $A \subseteq B$ y $B \subseteq A$ si y sólo si $A = B$.

(1), (2), (3) se expresan brevemente diciendo que la propiedad de contención es reflexiva, transitiva y antisimétrica, respectivamente.

En los Ejemplos 2.3 y 2.13 se mostró la existencia de dos útiles conjuntos; ahora hacemos una definición formal de ellos.

Definición 3.1 Si A y B son conjuntos, la *unión* de A y B, es el conjunto

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}.$$

La *intersección* de A y B es el conjunto

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\}.$$

Acorde a la definición anterior, una condición necesaria y suficiente para que $A \cap B \neq \emptyset$ es que A y B tengan elementos en común.

[1] Aquí consideraremos $\mathbf{N} = \{0, 1, 2, \ldots\}$.

Definición 3.2 Diremos que los conjuntos A y B son *ajenos* si $A \cap B = \emptyset$.

Con la terminología proporcionada por las definiciones anteriores podemos formular el Axioma de Fundación como sigue: "En cada conjunto no vacío A existe un elemento $u \in A$ que es ajeno a A, es decir, $u \cap A = \emptyset$".

El siguiente teorema nos muestra cómo se comportan la unión $\cup$ y la intersección $\cap$ con respecto de la contención.

Teorema 3.3 *Para cualesquiera conjuntos A, B, C, D tenemos:*

(a) $A \cap B \subseteq A \subseteq A \cup B$.

(b) Si $A \subseteq C$ y $B \subseteq D$ entonces $A \cap B \subseteq C \cap D$ y $A \cup B \subseteq C \cup D$.

(c) $A \subseteq C$ y $B \subseteq C$ si y sólo si $A \cup B \subseteq C$.

Demostración:

Solamente probaremos *(a)* dejando como ejercicio para el lector las partes *(b)* y *(c)*. Si $x \in A \cap B$ entonces $x \in A$ y $x \in B$, así en particular $x \in A$, es decir $A \cap B \subseteq A$. Por otra parte, para cualquier $x \in A$ se tiene que $x \in A \cup B$ por definición de $A \cup B$, es decir, $A \subseteq A \cup B$. ■

El siguiente teorema puede demostrarse sin dificultad.

Teorema 3.4 *Las operaciones $\cap$ y $\cup$ son:*

(a) Reflexivas: para todo A,

$$A \cap A = A = A \cup A.$$

(b) Asociativas:

$$A \cap (B \cap C) = (A \cap B) \cap C \quad y \quad A \cup (B \cup C) = (A \cup B) \cup C.$$

(c) Conmutativas:

$$A \cap B = B \cap A \quad y \quad A \cup B = B \cup A.$$

Más aún, $\cap$ distribuye sobre $\cup$ y $\cup$ distribuye sobre $\cap$:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

y

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

En virtud de la asociatividad, podemos designar a $A \cup (B \cup C)$ simplemente por $A \cup B \cup C$. Similarmente, una unión y una intersección de cuatro conjuntos, digamos $(A \cup B) \cup (C \cup D)$ y $(A \cap B) \cap (C \cap D)$, pueden ser escritas como $A \cup B \cup C \cup D$ y $A \cap B \cap C \cap D$ puesto que la distribución de paréntesis es irrelevante, y por la conmutatividad el orden de los términos también es irrelevante. Por inducción, la misma observación es aplicable a la unión y la intersección de cualquier número finito de conjuntos. La unión y la intersección de n conjuntos son escritas como

$$\bigcup_{k=1}^{n} A_k, \qquad \bigcap_{k=1}^{n} A_k.$$

Ahora daremos una caracterización de la propiedad $A \subseteq B$ en términos de la unión y la intersección.

Teorema 3.5 *Los siguientes enunciados son equivalentes:*
(a) $A \subseteq B$.
(b) $A = A \cap B$.
(c) $B = A \cup B$.

Demostración:

(a) $\Rightarrow$ *(b)*. Supongamos que $A \subseteq B$. Por 3.3(a) sabemos que $A \cap B \subseteq A$. Ahora, si $x \in A$ entonces $x \in A$ y $x \in B$ (ya que $A \subseteq B$); o sea, $x \in A \cap B$. Por lo tanto, $A \subseteq A \cap B$. Así concluimos que $A = A \cap B$.

(b) $\Rightarrow$ *(c)*. Si $A = A \cap B$ entonces se tienen las siguientes implicaciones: $x \in A \cup B \Rightarrow (x \in A) \vee (x \in B) \Rightarrow (x \in A \cap B) \vee (x \in B) \Rightarrow x \in B$, lo cual muestra que $A \cup B \subseteq B$, y nuevamente 3.3(a) nos proporciona $B \subseteq A \cup B$. Por lo tanto, $B = A \cup B$.

(c) $\Rightarrow$ *(a)*. Si $B = A \cup B$ entonces $A \subseteq A \cup B = B$. ■

Definición 3.6 La *diferencia* de dos conjuntos A y B es

$$A \setminus B = \{x \in A : x \notin B\}.$$

El Ejercicio 2.2.3 del capítulo anterior nos muestra que tal conjunto existe.

Ejemplo 3.7 Si $A = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$ y $B = \left\{x \in \mathbf{R} : \frac{1}{2} < x \leq 2\right\}$, entonces $A \setminus B = \left\{x \in \mathbf{R} : 0 \leq x \leq \frac{1}{2}\right\}$.

Ejemplo 3.8 $A \setminus \emptyset = A$ y $A \setminus B = A \setminus (A \cap B)$.

Ejemplo 3.9 Si $A \setminus B = A$, entonces $A \cap B = \emptyset$.

Ejemplo 3.10 $A \setminus B = \emptyset$ si y sólo si $A \subseteq B$.

La operación diferencia no tiene propiedades tan simples como $\cap$ y $\cup$; por ejemplo: si $A \neq \emptyset$, $(A \cup A) \setminus A \neq A \cup (A \setminus A)$, es decir, la colocación de paréntesis en $A \cup A \setminus A$ es importante. Otra diferencia es que, mientras que la unión y la intersección son operaciones conmutativas, por su propia definición la diferencia de conjuntos no es conmutativa.

Por otra parte, obsérvese que la negación de la proposición $x \in A \setminus B$, es equivalente a la proposición: $x \notin A \ \vee \ x \in B$, es decir, $x \notin A \setminus B$ si y sólo si x no es un elemento de A o x es un elemento de B. Ahora $x \in A \setminus (A \setminus B)$ si y sólo si $x \in A \wedge x \notin A \setminus B$ si y sólo si $[x \in A] \ \wedge \ [x \notin A \ \vee \ x \in B]$ si y sólo si $[x \in A \ \wedge x \notin A] \ \vee \ [x \in A \ \wedge \ x \in B]$ si y sólo si $x \in A \cap B$; hemos probado la siguiente proposición.

Proposición 3.11 *Para conjuntos arbitrarios A y B tenemos que*

$$A \cap B = A \setminus (A \setminus B).$$

Definición 3.12 Si $A \subseteq B$ el *complemento* de A *con respecto de* B es el conjunto $B \setminus A$.

Teorema 3.13 *Para cualesquiera dos conjuntos A y B, y cualquier conjunto E que contenga a $A \cup B$,*

$$A \setminus B = A \cap (E \setminus B).$$

Demostración:

Como $A \cup B \subseteq E$, tenemos que $A \setminus B = \{x \in E : (x \in A) \wedge (x \notin B\} = \{x \in E : x \in A\} \cap \{x \in E : x \notin B\} = A \cap (E \setminus B)$. ■

Teorema 3.14 *Si E es un conjunto que contiene a $A \cup B$, entonces:*

(a) $A \cap (E \setminus A) = \emptyset, \quad A \cup (E \setminus A) = E.$

(b) $E \setminus (E \setminus A) = A.$

(c) $E \setminus \emptyset = E, \quad E \setminus E = \emptyset.$

(d) $A \subseteq B$ *si y sólo si* $E \setminus B \subseteq E \setminus A.$

El siguiente es uno de los resultados elementales de mayor uso, se conoce habitualmente como *Leyes de De Morgan.*

Teorema 3.15 *Si $A, B \subseteq X$ entonces:*

(a) $X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B).$

(b) $X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$

DEMOSTRACIÓN:

$x \in X \setminus (A \cup B)$ si y sólo si $x \in X$ y $x \notin A \cup B$ si y sólo si $x \in X$, $x \notin A$ y $x \notin B$ si y sólo si $x \in X \setminus A$ y $x \in X \setminus B$. Esto establece *(a);* para probar *(b)* hacemos: $X \setminus [(X \setminus A) \cup (X \setminus B)] = [X \setminus (X \setminus A)] \cap [X \setminus (X \setminus B)] = A \cap B$; entonces $(X \setminus A) \cup (X \setminus B) = X \setminus (A \cap B)$. ■

Definición 3.16 Sean A y B conjuntos, se define la *diferencia simétrica* de A y B como:

$$A \triangle B = \{x \in A : x \notin B\} \cup \{x \in B : x \notin A\}.$$

En el Ejercicio 2.2.8 del capítulo anterior se pide demostrar que la diferencia simétrica de dos conjuntos existe.[2] La diferencia simétrica tiene las siguientes propiedades:

Teorema 3.17 *Para conjuntos A, B y C se tiene:*

(a) $A \triangle \emptyset = A$.
(b) $A \triangle A = \emptyset$.
(c) $A \triangle B = B \triangle A$.
(d) $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.
(e) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.
(f) Si $A \triangle B = A \triangle C$ *entonces* $B = C$.

Observemos además que, para cualesquiera dos conjuntos A y C existe - exactamente un conjunto B tal que $A \triangle B = C$, a saber, $B = A \triangle C$, en otras palabras:

$$A \triangle (A \triangle C) = C,$$
$$A \triangle B = C \quad \Rightarrow \quad B = A \triangle C.$$

En efecto, los incisos *(a), (b)* y *(d)* del Teorema 3.17 implican que $A \triangle (A \triangle C) = (A \triangle A) \triangle C = \emptyset \triangle C = C \triangle \emptyset = C$. Además si $A \triangle B = C$ entonces $A \triangle (A \triangle B) = A \triangle C$ y por tanto, $B = A \triangle C$. Lo anterior nos dice que la operación $\triangle$ es inversa de sí misma.

El lector que conozca la definición de anillo, utilizando el Teorema 3.4 en sus partes *(b)* y *(c)* referentes a la intersección y el Teorema 3.17, podrá darse cuenta que para cualquier conjunto X, el conjunto $\mathcal{P}(X)$ con las operaciones $\triangle$ y $\cap$ funcionando como suma y producto, es un anillo conmutativo con unidad X. Una peculiaridad de este anillo es que la operación "sustracción" coincide con la operación "suma" y más aún, el "cuadrado" de cualquier elemento es

[2] Las propiedades de la diferencia simétrica fueron investigadas extensivamente por Hausdorff en [H$_5$].

igual a ese elemento. Note que $\cup$ y $\setminus$ no funcionan como suma y sustracción, respectivamente.

Usando $\triangle$ y $\cap$ como las operaciones básicas, los cálculos en el álgebra de conjuntos pueden resolverse por aritmética ordinaria. Además, podemos omitir todos los exponentes y reducir todos los coeficientes módulo 2 (es decir, $2kA = \emptyset$ y $(2k+1)A = A$).

Este resultado es significativo puesto que las operaciones $\cup$ y $\setminus$ pueden ser expresadas en términos de $\triangle$ y $\cap$. Este hecho hace que toda el álgebra de subconjuntos de un conjunto particular X pueda ser representada como la aritmética en el anillo $\mathcal{P}(X)$. En efecto, uno puede fácilmente verificar que:

$$A \cup B = A \triangle B \triangle (A \cap B)$$
$$A \setminus B = A \triangle (A \cap B).$$

Ejercicios 3.1

1. Demuestre las partes (b) y (c) del Teorema 3.3.
2. Demuestre el Teorema 3.4.
3. (a) Demuestre que si $A \subseteq C$ entonces $A \cup (B \cap C) = (A \cup B) \cap C$.
   (b) ¿Será cierto el resultado anterior si se suprime la hipótesis $A \subseteq C$?
   (c) Demuestre que $A \subseteq C$ si y sólo si $A \cup (B \cap C) = (A \cup B) \cap C$.
4. Pruebe las afirmaciones hechas en los Ejemplos 3.8, 3.9 y 3.10.
5. Muestre que si $A \neq \emptyset$ entonces $(A \cup A) \setminus A \neq A \cup (A \setminus A)$.
6. Demuestre el Teorema 3.14.
7. Pruebe que
   (a) $A \setminus B = (A \cup B) \setminus B$.
   (b) $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
   (c) $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$.
   (d) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$.
   (e) $(A \setminus C) \cap (B \setminus C) = (A \cap B) \setminus C$.
   (f) $(A \setminus B) \setminus (A \setminus C) = A \cap (C \setminus B)$.

(g) $A_1 \cup A_2 \cup \cdots \cup A_n = (A_1 \setminus A_2) \cup \cdots \cup (A_{n-1} \setminus A_n) \cup (A_n \setminus A_1) \cup (\bigcap_{k=1}^{n} A_k)$.

(h) Si $A, B \subseteq X$, entonces $(X \setminus A) \setminus (X \setminus B) = B \setminus A$.

8. Muestre por medio de ejemplos que las siguientes proposiciones son falsas.

   (a) $A \setminus B = B \setminus A$.

   (b) $A \subseteq (B \cup C)$ implica $A \subseteq B$ o $A \subseteq C$.

   (c) $B \cap C \subseteq A$ implica $B \subseteq A$ o $C \subseteq A$.

9. Sea X un conjunto que contiene a $A \cup B$.

   (a) Demuestre que si $A \cup B = X$ entonces $X \setminus A \subseteq B$.

   (b) Demuestre que si $A \cap B = \emptyset$ entonces $A \subseteq X \setminus B$.

   (c) Utilizando los incisos anteriores demuestre que $A = X \setminus B$ si y sólo si $A \cup B = X$ y $A \cap B = \emptyset$.

10. Pruebe que el sistema de ecuaciones $A \cup X = A \cup B$, $A \cap X = \emptyset$ tiene a lo más una solución para X.

11. Sea A un conjunto. Demuestre que el "complemento" de A no es un conjunto. (El "complemento" de A es el conjunto de todos los $x \notin A$).

12. Pruebe el Teorema 3.17.

13. Pruebe que $A \triangle B = \emptyset$ si y sólo si $A = B$.

14. Pruebe que
$$A \cup B = A \triangle B \triangle (A \cap B)$$
$$A \setminus B = A \triangle (A \cap B).$$

3.2 Producto Cartesiano

Las operaciones de unión e intersección nos proporcionan nuevos conjuntos a partir de otros conjuntos dados. En esta sección introduciremos otro conjunto construido a partir de dos conjuntos A y B, que denotaremos por $A \times B$ y llamaremos el producto cartesiano de A y B. El producto cartesiano es una de las construcciones más importantes de la Teoría de Conjuntos, pues permite expresar muchos conceptos fundamentales de matemáticas en términos de conjuntos.

A diferencia de los elementos de la unión y de la intersección, los elementos del producto cartesiano son de naturaleza distinta a los elementos de A y de B, ya que $A \times B$ consistirá de lo que a continuación definiremos como parejas ordenadas de elementos. Intuitivamente una pareja ordenada es una entidad consistente de dos objetos en un orden específico. Para el empleo de la noción de par ordenado en matemáticas, uno desea que los pares ordenados tengan dos propiedades: *(i)* dados dos objetos a y b, exista un objeto, el cual puede ser denotado por (a, b) que esté unívocamente determinado por a y b; *(ii)* si (a, b) y (c, d) son dos pares ordenados, entonces $(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$. Por el Ejemplo 2.35, es posible definir un objeto, de hecho un conjunto, con la propiedad *(i)*.

Definición 3.18 Se define el *par ordenado* de elementos a y b como

$$(a, b) = \{\{a\}, \{a, b\}\}.$$

Si $a \neq b$, (a, b) tiene dos elementos, un singular $\{a\}$ y un par no ordenado $\{a, b\}$. La *primera coordenada* de (a, b) es el elemento que pertenece a ambos conjuntos, o sea a, y la *segunda coordenada* es el elemento perteneciente a sólo uno de los conjuntos, a saber, b. Si $a = b$, entonces $(a, a) = \{\{a\}, \{a, a\}\}$ tiene un único elemento; en este caso ambas coordenadas son iguales. Es muy oportuno observar que $(a, b) \subseteq \mathcal{P}(\{a, b\})$.

Probaremos ahora que los pares ordenados tienen la propiedad *(ii)* antes mencionada.

Teorema 3.19 *$(a, b) = (c, d)$ si y sólo si $a = c$ y $b = d$.*

Demostración:

$\Leftarrow$] Si $a = c$ y $b = d$, entonces:

$$(a, b) = \{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\} = (c, d).$$

$\Rightarrow$] Supongamos que $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Si $a \neq b$, entonces debe suceder que $\{a\} = \{c\}$ y $\{a, b\} = \{c, d\}$. Así, $a = c$, y entonces $\{a, b\} = \{a, d\}$. De esto se deduce que $b = d$. Si $a = b$, $\{\{a\}, \{a, b\}\} = \{\{a\}\}$. Así $\{a\} = \{c\}$ y $\{a\} = \{c, d\}$, lo cual implica que $a = c = d$. Por lo tanto, $a = c$ y $b = d$. ■

Con los pares ordenados a nuestra disposición podemos definir ternas ordenadas como

$$(a, b, c) = ((a, b), c),$$

cuartetas ordenadas como

$$(a, b, c, d) = ((a, b, c), d),$$

etc.; y es evidente que la correspondiente caracterización (Teorema 3.19) de igualdad también es apropiada.

Kuratowski [K_6] en 1921 fue el primero en dar una definición satisfactoria de par ordenado. Lo complicado de tal definición reside en evitar toda referencia a la forma de escribir los símbolos (a, b). Los filósofos de la primera época de la Teoría de Conjuntos se encontraron metidos en un problema en lo relativo a dicha cuestión. La dificultad reside en eliminar la simetría existente entre a y b. El motivo por el cual los filósofos no consiguieron hacerlo fue su confusión en cuanto a la distinción que existe entre x y $\{x\}$, pues querían que fuese lo mismo. Poniendo $(a, b) = \{\{a\}, \{a, b\}\}$, la asimetría del segundo miembro basta para probar el Teorema 3.19, el cual hace que la definición de par ordenado sea adecuada.

Definición 3.20 Sean A y B conjuntos cualesquiera. El *producto cartesiano* de A y de B es el conjunto $A \times B$ es el conjunto consistente de todos aquellos pares ordenados (a, b) tales que $a \in A$ y $b \in B$, esto es,

$$A \times B = \{(a, b) : a \in A \ \wedge \ b \in B\}.$$

Estamos describiendo un nuevo conjunto y por ende debemos asegurar su existencia como tal, es por ello que damos la siguiente proposición que nos afirma que $A \times B$ es un conjunto.

Proposición 3.21 *Para cualesquiera A y B, $A \times B$ es un conjunto.*

Demostración:

Por el Ejemplo 2.27 del Capítulo 2 tenemos que siempre que $a \in A$ y $b \in B$ entonces $\mathcal{P}(\{a, b\}) \subseteq \mathcal{P}(A \cup B)$, y como $(a, b) \subseteq \mathcal{P}(\{a, b\})$, se sigue que cuando $a \in A$ y $b \in B$ se tiene que $(a, b) \subseteq \mathcal{P}(A \cup B)$, o bien $(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B))$. Por lo tanto,

$$A \times B = \{(a, b) \in \mathcal{P}(\mathcal{P}(A \cup B)) : a \in A \ \wedge \ b \in B\}.$$

Ya que $\mathcal{P}(\mathcal{P}(A \cup B))$ existe, la existencia de $A \times B$ como conjunto se sigue del Axioma Esquema de Comprensión. ■

Denotaremos $A \times A$ por A^2. Hemos definido una terna ordenada de elementos $a,\ b$ y c como $(a, b, c) = ((a, b), c)$. Para ser consistentes con esa definición, introducimos el producto cartesiano de tres conjuntos $A,\ B$ y C como

$$A \times B \times C = (A \times B) \times C.$$

Note que

$$A \times B \times C = \{(a, b, c) : a \in A \ \wedge \ b \in B \ \wedge \ c \in C\}.$$

Usando una obvia extensión de nuestra notación, $A \times A \times A$ será denotado por A^3. De modo análogo, el producto cartesiano de cuatro conjuntos puede también ser introducido.

Ejemplo 3.22 Sean $A = \{1, 2, 3\}$ y $B = \{2, 4, 5\}$. Entonces

$$A \times B = \{(1, 2),\ (1, 4),\ (1, 5),\ (2, 2),\ (2, 4),\ (2, 5),\ (3, 2),\ (3, 4),\ (3, 5)\}.$$

Ejemplo 3.23 Si $A = \mathbf{R} = B$, entonces $A \times B = \{(x, y) : x, y \in \mathbf{R}\} = \mathbf{R}^2$ es el plano usual de la geometría analítica.

Ejemplo 3.24 Sea $A = \left\{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\right\}$ (es decir, A es la circunferencia unitaria) y sea $B = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$. Entonces, $A \times B$ es el conjunto de los puntos de $\mathbf{R}^3$ que están en el cilindro unitario de altura 1.

Teorema 3.25 *(a) $A \times B = \emptyset$ si y sólo si $A = \emptyset$ o $B = \emptyset$.*
(b) Si $C \times D \neq \emptyset$, entonces $C \times D \subseteq A \times B$ si y sólo si $C \subseteq A$ y $D \subseteq B$.
(c) $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
(d) $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Demostración:

La demostración de la proposición en *(a)* es inmediata a partir de las definiciones.

(b) $\Rightarrow$] Veamos que $D \subseteq B$. Un argumento simétrico será suficiente para establecer $C \subseteq A$. Puesto que $C \times D \neq \emptyset$, aplicando *(a)* obtenemos que $C \neq \emptyset$. Fijemos un $c \in C$ arbitrario. Ahora, deseamos demostrar que para todo x, $x \in D \Rightarrow x \in B$. Sea $x \in D$. Entonces $(c, x) \in C \times D$ y luego $(c, x) \in A \times B$. De aquí se sigue que $x \in B$. Por lo tanto $D \subseteq B$.

$\Leftarrow$] Sea $(c, d) \in C \times D$. Entonces $c \in C$ y $d \in D$. Como por hipótesis $C \subseteq A$ y $D \subseteq B$, se tiene que $c \in A$ y $d \in B$; de aquí $(c, d) \in A \times B$. Por lo tanto, $C \times D \subseteq A \times B$.

(c) $(x, y) \in A \times (B \cup C)$ si y sólo si $x \in A$ y $y \in B \cup C$ si y sólo si $x \in A$ y $y \in B$ o $y \in C$ si y sólo si $x \in A$ y $y \in B$ o bien $x \in A$ y $y \in C$ si y sólo si $(x, y) \in A \times B$ o $(x, y) \in A \times C$ si y sólo si $(x, y) \in (A \times B) \cup (A \times C)$.
(d) Ejercicio. ■

Para conjuntos no vacíos A y B se tiene que $A \times B = B \times A$ si y sólo si $A = B$; así, la operación producto cartesiano no es conmutativa.

Ejercicios 3.2

1. Pruebe que $(a, b) \subseteq \mathcal{P}(\{a, b\})$.
2. Pruebe que (a, b), (a, b, c) y (a, b, c, d) existen para todo a, b, c y d.
3. Pruebe que $(a, b, c) = (a', b', c')$ si y sólo si $a = a'$, $b = b'$ y $c = c'$.
4. Encuentre a, b y c tales que $((a, b), c) \neq (a, (b, c))$. A pesar de este resultado, puede definirse la terna ordenada de elementos a, b y c como $(a, b, c) = (a, (b, c))$, y el producto cartesiano de A, B y C como $A \times B \times C = A \times (B \times C)$. Más adelante veremos que en términos conjuntistas esta discrepancia es irrelevante.
5. Demuestre que $A \times B = B \times A$ si y sólo si $A = B$.
6. Muestre que
   (a) $A \times (B \times C) \neq (A \times B) \times C$.
   (b) $A^3 \neq A \times A^2$, es decir, $(A \times A) \times A \neq A \times (A \times A)$.
   Este ejercicio muestra que $\times$ no es asociativo.
7. Si A, B son conjuntos no vacíos y $(A \times B) \cup (B \times A) = C \times C$, demuestre que $A = B = C$.
8. Pruebe la parte (d) del Teorema 3.25.
9. Demuestre que:
   (a) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.
   (b) $(A \cap B) \times C = (A \times C) \cap (B \times C)$.

(c) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

(d) $A \times (B \triangle C) = (A \times B) \triangle (A \times C)$.

10. Sean $A, B \subseteq X$ y $C, D \subseteq Y$. Demuestre que:

(a) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.

(b) $(A \times C) \cup (B \times D) \subseteq (A \cup B) \times (C \cup D)$. Muestre que es posible que no se dé la igualdad.

(c) $(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D) \cup (A \times D) \cup (B \times C)$.

(d) $(X \times Y) \setminus (B \times C) = ((X \setminus B) \times Y) \cup (X \times (Y \setminus C)$.

11. Para dos conjuntos A y B, se define la *unión ajena* de A y B como: $A \sqcup B = (A \times \{x\}) \cup (B \times \{y\})$, donde $x \notin B$, $y \notin A$. Demuestre el análogo del Teorema 3.4 para uniones ajenas.

3.3 Familias de Conjuntos

En el párrafo que sigue al Axioma de Unión hablamos de un tipo muy especial de conjuntos: los *sistemas* o *familias* de conjuntos. Estos conjuntos (como otros) tienen como elementos a conjuntos, es decir, una familia de conjuntos es un "conjunto de conjuntos". Las familias de conjuntos juegan un papel destacado en otras ramas de las matemáticas, donde el objetivo es estudiar a familias especiales de conjuntos. Por ejemplo, la Topología no es otra cosa que el estudio de las propiedades un sistema especial de subconjuntos de un conjunto dado X. La terminología sistema o familia de conjuntos tiene por objeto resaltar el hecho de que trataremos a los elementos de la familia como conjuntos mismos. Usualmente denotaremos a las familias de conjuntos con letras mayúsculas caligráficas tales como $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{X}$, $\mathcal{Z}$. Veamos algunos ejemplos.

Ejemplo 3.26 $\mathcal{A} = \{\emptyset, \{\emptyset\}\}$ es un sistema de conjuntos cuyos elementos son el conjunto vacío $\emptyset$ y el conjunto unitario $\{\emptyset\}$.

Ejemplo 3.27 Sea $\mathcal{M} = \{\{x \in \mathbf{N} : x \text{ es par}\}, \{x \in \mathbf{N} : x \text{ es impar}\}\}$. Entonces $\mathcal{M}$ es un sistema de conjuntos cuyos elementos son el conjunto de los números naturales pares y el conjunto de los números naturales impares. Obsérvese que $\mathbf{N} \neq \mathcal{M}$.

Ejemplo 3.28 Para cualquier conjunto X, el conjunto potencia de X, $\mathcal{P}(X)$, es la familia de todos los subconjuntos de X.

Ejemplo 3.29 Recuerde que a una circunferencia en $\mathbf{R}^2$ con centro en el punto $x \in \mathbf{R}^2$ y radio $r > 0$, la podemos considerar como el conjunto $C(x,r) = \left\{y \in \mathbf{R}^2 : \|x - y\| = r\right\}$. Sea E_x la familia de todas las circunferencias en $\mathbf{R}^2$ con centro $x \in \mathbf{R}^2$, es decir, $E_x = \{C(x,r) : r > 0\}$, y sea $\mathcal{E} = \left\{E_x : x \in \mathbf{R}^2\right\}$. Entonces $\mathcal{E}$ es un sistema de conjuntos cuyos elementos son familias de conjuntos. Note que ni los puntos de $\mathbf{R}^2$, ni las circunferencias son elementos de $\mathcal{E}$.

El Axioma de Unión y el Axioma Esquema de Comprensión (véase el párrafo que sigue al Ejemplo 2.15) dan posibilidad de la siguiente definición.

Definición 3.30 Sea $\mathcal{F}$ es una familia no vacía de conjuntos.

(a) La *unión de la familia* $\mathcal{F}$ es el conjunto

$$\bigcup \mathcal{F} = \bigcup_{A \in \mathcal{F}} A = \{x : \exists A \in \mathcal{F}, x \in A\}.$$

(b) La *intersección de la familia* $\mathcal{F}$ es el conjunto

$$\bigcap \mathcal{F} = \bigcap_{A \in \mathcal{F}} A = \{x : \forall A \in \mathcal{F}, x \in A\}.$$

Ejemplo 3.31 Si $\mathcal{M}$ es la familia definida en el Ejemplo 3.27, entonces $\mathbf{N} = \bigcup \mathcal{M}$.

Ejemplo 3.32 Para cualquier conjunto X, $X = \bigcup \mathcal{P}(X)$.

Ejemplo 3.33 Si $\mathcal{F} = \{A, B\}$, entonces $\bigcup \mathcal{F} = A \cup B$ y $\bigcap \mathcal{F} = A \cap B$. Ver Ejemplo 2.13.

Ejemplo 3.34 Si $\mathcal{F} = \{A\}$, entonces $\bigcup \mathcal{F} = A = \bigcap \mathcal{F}$.

A continuación introduciremos un concepto asociado con las familias de conjuntos. Supongamos que tomamos un conjunto $I \neq \emptyset$ y que a cada $\alpha \in I$ le corresponde un único conjunto A_α. Al sistema $\mathcal{A} = \{A_\alpha : \alpha \in I\}$ le llamamos *familia de conjuntos indizada* por el conjunto I. En este caso, se dice que I es el conjunto de índices de $\mathcal{A}$. Nótese que no se requiere que a distintos índices les correspondan distintos conjuntos. Para referirnos a familias indizadas de conjuntos, en ocasiones emplearemos la forma breve $\{A_\alpha\}_{\alpha \in I}$, o simplemente $\{A_\alpha\}_\alpha$ cuando sea claro el conjunto de índices que se está usando.

Observación 3.35 Cualquier familia no vacía de conjuntos $\mathcal{F}$ puede considerarse como una familia indizada de conjuntos, donde el conjunto de índices es *el mismo* $\mathcal{F}$, a saber: $\mathcal{F} = \{F_A : A \in \mathcal{F}\}$, donde $F_A = A$ para cada $A \in \mathcal{F}$.

Ejemplo 3.36 Sean $I = \{1, 2, 3\}$ y $A_1 = \{1, 2, 5\}$, $A_2 = \{5, 7, 1\}$, $A_3 = \{2, 5, 7\}$. Entonces $\mathcal{A} = \{A_i\}_{i \in I}$ es una familia indizada de conjuntos.

Ejemplo 3.37 Para $x \in \mathbf{R}^2$, la familia E_x del Ejemplo 3.29 es una familia indizada de conjuntos, donde el conjunto de índices es el conjunto de los números reales positivos $I = \{r \in \mathbf{R} : r > 0\}$. También el sistema $\mathcal{E}$ es una familia indizada de conjuntos, aquí el conjunto de índices es $\mathbf{R}^2$.

Con el concepto de familia indizada de conjuntos, la unión de la familia $\mathcal{F} = \{A_\alpha\}_{\alpha \in I}$ puede denotarse como

$$\bigcup \mathcal{F} = \bigcup \{A_\alpha : \alpha \in I\} = \bigcup \{A_\alpha\}_{\alpha \in I} = \bigcup_{\alpha \in I} A_\alpha$$

y es el conjunto $\{x : \exists \alpha \in I \text{ tal que } x \in A_\alpha\}$. La intersección es denotada por

$$\bigcap \mathcal{F} = \bigcap \{A_\alpha : \alpha \in I\} = \bigcap \{A_\alpha\}_{\alpha \in I} = \bigcap_{\alpha \in I} A_\alpha$$

y es el conjunto $\{x : \forall \alpha \in I,\ x \in A_\alpha\}$. Cuando el conjunto de índices sea el conjunto de los números naturales $\mathbf{N}$, denotaremos con

$$\bigcup_{n=0}^{\infty} A_n \quad \text{a} \quad \bigcup_{n \in \mathbf{N}} A_n$$

y con

$$\bigcap_{n=0}^{\infty} A_n \quad \text{a} \quad \bigcap_{n \in \mathbf{N}} A_n.$$

Ejemplo 3.38 Para cualquier conjunto X, $X = \bigcup \{\{x\} : x \in X\}$.

Ejemplo 3.39 Sea $A_k = \{n \in \mathbf{N} : n \geq k\}$, $k = 0, 1, 2, 3, \ldots$. Note que $A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots$, y que $\bigcap_{k=0}^{\infty} A_k = \emptyset$.

Ejemplo 3.40 Sean $x \in \mathbf{R}^2$ y E_x la familia indizada de conjuntos definida en el Ejemplo 3.29. Entonces $\bigcup E_x = \bigcup_{r>0} C(x, r) = \mathbf{R}^2 \setminus \{x\}$ *y* $\bigcap E_x = \bigcap_{r>0} C(x, r) = \emptyset$.

Ejemplo 3.41 Si

$$\mathcal{C} = \big\{C \in \mathcal{P}(\mathbf{R}^2) : C\text{es una circunferencia no degenerada}\big\}$$

y $\mathcal{E}$ es el sistema del Ejemplo 3.29, entonces $\mathcal{C} = \bigcup \mathcal{E}$.

Ejemplo 3.42 Si $\mathcal{A} \subseteq \mathcal{B}$ entonces $\bigcap \mathcal{B} \subseteq \bigcap \mathcal{A}$.

No hay problema con la Definición 3.30 si uno de los elementos de $\mathcal{F}$ es el conjunto vacío. Por otra parte el Ejemplo 2.12 muestra que si $\mathcal{F} = \emptyset$ entonces $\bigcup \mathcal{F} = \emptyset$; en efecto, aplicando literalmente el Axioma de Unión, vemos que no existen x que satisfagan la propiedad que define a la unión de la familia $\mathcal{F}$. Sin embargo, en el caso en que $\mathcal{F} = \emptyset$ no es posible definir a la intersección de $\mathcal{F}$ pues esto generaría contradicciones dado que cualquier x satisface la propiedad que define a la intersección de $\mathcal{F}$, es decir, $x \in A$ para todo $A \in \mathcal{F}$ (puesto que no hay tales A). Así $\bigcap \emptyset$ podría ser el "conjunto de todos los conjuntos", por lo cual la *intersección de una familia vacía de conjuntos no está definida.* Por las observaciones anteriores y 3.35, restringiremos el estudio a familias indizadas no vacías de conjuntos. El siguiente teorema nos proporciona propiedades que relacionan a las uniones e intersecciones "generalizadas" con las uniones e intersecciones "elementales", la generalización de las Leyes de De Morgan y el producto cartesiano.

Teorema 3.43 *(a)* $\bigcup_\alpha$ *distribuye sobre* $\cap$ *y* $\bigcap_\alpha$ *distribuye sobre* $\cup$.

$$\left[\bigcup_{\alpha\in I} A_\alpha\right] \cap \left[\bigcup_{\beta\in J} B_\beta\right] = \bigcup \{A_\alpha \cap B_\beta : (\alpha,\beta) \in I \times J\} \tag{3.3.1}$$

$$\left[\bigcap_{\alpha\in I} A_\alpha\right] \cup \left[\bigcap_{\beta\in J} B_\beta\right] = \bigcap \{A_\alpha \cup B_\beta : (\alpha,\beta) \in I \times J\}. \tag{3.3.2}$$

(b) Si el complemento es tomado respecto a X*, entonces:*

$$X \setminus \bigcup \{A_\alpha : \alpha \in I\} = \bigcap \{X \setminus A_\alpha : \alpha \in I\} \tag{3.3.3}$$

$$X \setminus \bigcap \{A_\alpha : \alpha \in I\} = \bigcup \{X \setminus A_a : \alpha \in I\}. \tag{3.3.4}$$

(c) $\bigcup_\alpha$ *y* $\bigcap_\alpha$ *distribuyen sobre el producto cartesiano:*

$$\left[\bigcup_{\alpha\in I} A_\alpha\right] \times \left[\bigcup_{\beta\in J} B_\beta\right] = \bigcup \{A_\alpha \times B_\beta : (\alpha,\beta) \in I \times J\} \tag{3.3.5}$$

$$\left[\bigcap_{\alpha\in I} A_\alpha\right] \times \left[\bigcap_{\beta\in J} B_\beta\right] = \bigcap \{A_\alpha \times B_\beta : (\alpha,\beta) \in I \times J\}. \tag{3.3.6}$$

DEMOSTRACIÓN:

(a) $x \in [\bigcup\{A_\alpha : \alpha \in I\}] \cap [\bigcup\{B_\beta : \beta \in J\}]$ si y sólo si $x \in \bigcup_{\alpha\in I} A_\alpha$ y $x \in \bigcup_{\beta\in J} B_\beta$ si y sólo si $x \in A_{\alpha_o}$ para algún $\alpha_o \in I$ y $x \in B_{\beta_o}$ para algún $\beta_o \in J$ si y sólo si $x \in A_{\alpha_o} \cap B_{\beta_0}$ si y sólo si $x \in \bigcup\{A_\alpha \cap B_\beta : (\alpha, \beta) \in I \times J\}$. Esto establece la igualdad (3.3.1). Similarmente se establece (3.3.2).

(b) $x \in X \setminus \bigcup\{A_\alpha : \alpha \in I\}$ si y sólo si $x \in X$ y $x \notin \bigcup_{\alpha\in I} A_\alpha$ si y sólo si $x \in X$ y $\forall\alpha \in I,\ x \notin A_\alpha$ si y sólo si $x \in X \setminus A_\alpha$ para cada $\alpha \in I$, si y sólo si $x \in \bigcap\{X \setminus A_\alpha : \alpha \in I\}$. Esto establece la ecuación (3.3.3). Análogamente se establece (3.3.4).

(c) $(a, b) \in [\bigcup\{A_\alpha : \alpha \in I\}] \times [\bigcup\{B_\beta : \beta \in J\}]$ si y sólo si existen $\alpha \in I$ y $\beta \in J$ tales que $a \in A_\alpha$ y $b \in B_\beta$ si y sólo si $(a, b) \in A_\alpha \times B_\beta$ si y sólo si $(a, b) \in \bigcup\{A_\alpha \times B_\beta : (\alpha, \beta) \in I \times J\}$. Lo que establece la igualdad (3.3.5). Del mismo modo se prueba (3.3.6). ■

El siguiente corolario establece formas más concretas del teorema anterior, las cuales son usadas con mayor frecuencia.

Corolario 3.44 *(a)* $A \cap \bigcup\{A_\alpha : \alpha \in I\} = \bigcup\{A \cap A_\alpha : \alpha \in I\}$.
(b) $A \cup \bigcap\{A_\alpha : \alpha \in I\} = \bigcap\{A \cup A_\alpha : \alpha \in I\}$.
(c) $A \times \bigcup\{A_\alpha : \alpha \in I\} = \bigcup\{A \times A_\alpha : \alpha \in I\}$.
(d) $A \times \bigcap\{A_\alpha : \alpha \in I\} = \bigcap\{A \times A_\alpha : \alpha \in I\}$.

Finalmente:

Teorema 3.45 $\bigcap_\alpha$ *y* $\mathcal{P}$ *conmutan*

$$\bigcap_{\alpha\in I} \mathcal{P}(A_\alpha) = \mathcal{P}\left(\bigcap_{\alpha\in I} A_\alpha\right).$$

Sin embargo, $\bigcup_\alpha$ *y* $\mathcal{P}$ *no conmutan, aunque*

$$\bigcup_{\alpha\in I} \mathcal{P}(A_\alpha) \subseteq \mathcal{P}\left(\bigcup_{\alpha\in I} A_\alpha\right).$$

DEMOSTRACIÓN:

$A \in \bigcap_{\alpha\in I} \mathcal{P}(A_\alpha)$ si y sólo si para cada $\alpha \in I,\ A \in \mathcal{P}(A_\alpha)$ si y sólo si para cada $\alpha \in I$, $A \subseteq A_\alpha$ y sólo si $A \subseteq \bigcap_{\alpha\in I} A_\alpha$ si y sólo si $A \in \mathcal{P}\left(\bigcap_{\alpha\in I} A_\alpha\right)$.

Si $A \in \bigcup_{\alpha\in I} \mathcal{P}(A_\alpha)$ entonces existe $\alpha \in I$ tal que $A \in \mathcal{P}(A_\alpha)$, o sea, $A \subseteq A_\alpha \subseteq \bigcup_{\alpha\in I} A_\alpha$, lo que implica $A \in \mathcal{P}\left(\bigcup_{\alpha\in I} A_\alpha\right)$.

Para ver que $\bigcup_\alpha$ y $\mathcal{P}$ no conmutan, sean $A_1 = \{1\}$, $A_2 = \{2\}$. Entonces

$$\bigcup_{\alpha \in I} \mathcal{P}(A_\alpha) = \{\emptyset, \{1\}, \{2\}\}$$

y

$$\mathcal{P}\left(\bigcup_{\alpha \in I} A_\alpha\right) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}. \quad \blacksquare$$

Ejercicios 3.3

1. Sea $\mathcal{M} = \{\{x \in \mathbf{N} : x \text{ es par}\}, \{x \in \mathbf{N} : x \text{ es impar}\}\}$. Muestre que $\mathcal{M} \neq \mathbf{N}$ y que $\mathbf{N} = \bigcup \mathcal{M}$.

2. Suponiendo que $\mathbf{R}$ es un conjunto, demuestre que los conjuntos definidos en el Ejemplo 3.29 existen.

3. Demuestre que $\bigcap \mathcal{F}$ existe para toda $\mathcal{F} \neq \emptyset$. ¿Dónde se utiliza la hipótesis $\mathcal{F} \neq \emptyset$ en la demostración?

4. Muestre que para cualquier conjunto X, $\bigcap \mathcal{P}(X) = \emptyset$.

5. Sea $\mathcal{F}$ una familia de conjuntos. Pruebe que $\bigcup \mathcal{F} = \emptyset$ si y sólo si $\mathcal{F} = \emptyset$ o $A \in \mathcal{F}$ implica $A = \emptyset$.

6. Verifique las afirmaciones de los Ejemplos 3.40, 3.41 y 3.42.

7. Si A y B son conjuntos y X es el par ordenado (A, B), pruebe lo siguiente:

   (a) $\bigcup X = \{A, B\}$.
   (b) $\bigcap X = \{A\}$.
   (c) $\bigcup (\bigcap X) = A$.
   (d) $\bigcap (\bigcap X) = A$.
   (e) $\bigcup (\bigcup X) = A \cup B$.
   (f) $\bigcap (\bigcup X) = A \cap B$.

8. Supóngase que se sabe que la familia X es un par ordenado. Use los resultados del ejercicio anterior para obtener la primera y la segunda coordenadas de X.

9. Pruebe las ecuaciones (3.3.2), (3.3.4) y (3.3.6) del Teorema 3.43.

10. Una familia de conjuntos $\mathcal{F}$ se dice *ajena por pares* si para cualesquiera $A, B \in \mathcal{F}$, con $A \neq B$, se tiene que $A \cap B = \emptyset$. Sea $\mathcal{F} = \{A_n : n \in \mathbf{N}\}$ una familia de conjuntos ajena por pares, y sea $S_n = \bigcup_{k=0}^{n} A_k$ para $n = 0, 1, 2, 3, \ldots$.

    (a) Muestre que la familia

    $$\mathcal{E} = \{A_0\} \cup \{A_n \setminus S_{n-1} : n \in \mathbf{N} \text{ y } n \geq 1\}$$

    es ajena por pares.

    (b) Muestre que $\bigcup_{n=0}^{\infty} A_n = \bigcup \mathcal{E} = A_0 \cup (A_1 \setminus S_2) \cup \cdots \cup (A_n \setminus S_{n-1}) \cup \cdots$.

11. Sean $\mathcal{F} \neq \emptyset$ y X conjuntos.

    (a) Sea $\mathcal{E}_1 = \{A \in \mathcal{P}(X) : A = F \cap X \text{ para algún } F \in \mathcal{F}\}$. Pruebe que $X \cap \bigcup \mathcal{F} = \bigcup \mathcal{E}_1$.

    (b) Sea $\mathcal{E}_2 = \{A \in \mathcal{P}(X) : A = X \setminus F \text{ para algún } F \in \mathcal{F}\}$. Pruebe que $X \setminus \bigcup \mathcal{F} = \bigcap \mathcal{E}_2$, $X \setminus \bigcap \mathcal{F} = \bigcup \mathcal{E}_2$.

12. Demuestre que la unión y la intersección generalizada satisfacen la siguiente forma de asociación:

    $$\bigcup \Big\{ A_\alpha : \alpha \in \bigcup \mathcal{I} \Big\} = \bigcup_{I \in \mathcal{I}} \left(\bigcup_{\alpha \in I} A_\alpha \right)$$

    $$\bigcap \Big\{ A_\alpha : \alpha \in \bigcap \mathcal{I} \Big\} = \bigcap_{I \in \mathcal{I}} \left(\bigcap_{\alpha \in I} A_\alpha \right),$$

    donde $\mathcal{I}$ es una familia no vacía de conjuntos no vacíos.

13. Sea $\mathcal{F} = \{A_n : n \in \mathbf{N} \setminus \{0\}\}$ una familia de subconjuntos de X, es decir, $\mathcal{F} \subseteq \mathcal{P}(X)$. Defina

    $$\limsup A_n = \bigcap_{n=1}^{\infty} \left(\bigcup_{k=0}^{\infty} A_{n+k} \right),$$

    $$\liminf A_n = \bigcup_{n=1}^{\infty} \left(\bigcap_{k=0}^{\infty} A_{n+k} \right).$$

    Sea también para cada $x \in X$, $J_x = \{n \in \mathbf{N} : x \in A_n\}$. Demuestre lo siguiente:

(a) $\limsup A_n = \{x \in X : J_x \text{ es infinito}\}$.

(b) $\liminf A_n = \{x \in X : \mathbf{N} \setminus J_x \text{ es finito}\}$.

(c) $\bigcap_{n=1}^{\infty} A_n \subseteq \liminf A_n \subseteq \limsup A_n \subseteq \bigcup_{n=1}^{\infty} A_n$.

(d) $\liminf(X \setminus A_n) = X \setminus \limsup A_n$.

(e) Si $\{B_n\}_{n\in\mathbf{N}}$ es otra familia de subconjuntos de X entonces:

i. $\liminf A_n \cup \liminf B_n \subseteq \liminf(A_n \cup B_n)$.

ii. $\liminf A_n \cap \liminf B_n = \liminf(A \ln \cap B_n)$.

iii. $\limsup(A_n \cap B_n) \subseteq \limsup A_n \cap \limsup B_n$.

iv. $\limsup(A_n \cup B_n) = \limsup A_n \cup \limsup B_n$.

(f) Si $A_1 \subseteq A_2 \subseteq \cdots$ o $A_1 \supseteq A_2 \supseteq \cdots$, entonces $\liminf A_n = \limsup A_n$.

4

Relaciones y Funciones

Los conceptos de relación y función son, sin duda alguna, de los más importantes dentro de las matemáticas modernas. La mayor parte de la investigación en matemáticas se centra en el estudio de relaciones y funciones, por lo cual, no ha de sorprender que estos conceptos sean de una gran generalidad. Hausdorff consideraba que el concepto de función es casi tan primitivo como el de conjunto, y qué decir del concepto de relación, el cual intuitivamente parece más esencial que el de función.

En matemáticas la palabra *relación* es usada en el sentido de relacionar. Las siguientes oraciones parciales son ejemplos de relaciones:

es menor que,	está incluido en,
divide a,	es miembro de,
es congruente a,	es madre de.

En este capítulo enfocaremos conceptos como los de orden y función desde el punto de vista conjuntista. Veremos que estos pueden ser tratados como relaciones, y que las relaciones pueden ser definidas de manera natural como conjuntos de una estructura especial.

4.1 Relaciones

Empleando parejas ordenadas, intuitivamente podemos pensar que una relación (binaria) R es una proposición tal que, para cada par ordenado (a, b), uno puede determinar cuándo a está en relación R con b o cuándo no lo está. Parece factible que toda relación debe determinar de manera única al conjunto de aquellas parejas ordenadas en las cuales la primera coordenada mantiene esta relación con la segunda. Si conocemos la relación, conocemos el conjunto y, mejor aún, si conocemos el conjunto, conocemos la relación. En otras palabras, las relaciones pueden ser representadas como el conjunto de todos los pares ordenados de objetos mutuamente relacionados. Por ejemplo, el conjunto de todos los pares ordenados consistente de un número real y su raíz puede ser llamado la relación raíz cuadrada. Nótese aquí la importancia de considerar

pares ordenados y no sólo pares no ordenados.

Quizá no sepamos lo que es una relación, pero sabemos lo que es un conjunto y las consideraciones precedentes establecen una estrecha conexión entre relaciones y conjuntos. El estudio preciso de las relaciones en la Teoría de Conjuntos saca provecho de esta conexión heurística; lo más fácil de hacer es definir una relación como el conjunto de parejas ordenadas que determina.

Definición 4.1 Un conjunto R es una *relación (binaria)* si todo elemento de R es un par ordenado, es decir, si para todo $z \in R$, existen x, y tales que $z = (x, y)$. Si $R \subseteq A \times B$ diremos que R *es una relación de* A *en* B, o *entre* A *y* B; y si $R \subseteq A \times A$ diremos simplemente que R *es una relación en* A.

Ejemplo 4.2 Definimos una relación entre los enteros positivos y los enteros, diciendo que un entero positivo m está en relación R con un entero n, si m divide a n. La relación R es simplemente el conjunto

$$\{z : \exists\, m, n \text{ tales que } z = (m, n),\ m \in \mathbf{Z},\ n \in \mathbf{Z},\ m > 0 \text{ y } m \text{ divide a } n\}.$$

Los elementos de R son pares ordenados

$$\begin{gathered}
\ldots,\ (1,-3),\ (1,-2),\ (1,-1),\ (1,0),\ (1,1),\ (1,2),\ (1,3),\ldots \\
\ldots,\ (2,-6),\ (2,-4),\ (2,-2),\ (2,0),\ (2,2),\ (2,4),\ (2,6),\ldots \\
\ldots,\ (3,-9),\ (3,-6),\ (3,-3),\ (3,0),\ (3,3),\ (3,6),\ (3,9),\ldots \\
\ldots
\end{gathered}$$

Ejemplo 4.3 Sean A y B conjuntos. La relación de A en B de todos los pares ordenados (a, b) con $a \in A$ y $b \in B$ es llamada relación producto cartesiano y es denotada por $A \times B$.

Ejemplo 4.4 El conjunto $\emptyset$ es una relación llamada relación vacía (para demostrar que $\emptyset$ es un conjunto de parejas ordenadas, busque un elemento de $\emptyset$ que no sea una pareja ordenada).

Ejemplo 4.5 Para cualquier conjunto A, la diagonal

$$Id_A = \{(a, a) : a \in A\}$$

es la *relación de igualdad* o *relación identidad*. Note que en una relación en A (como Id_A) cada par de elementos en A no necesariamente están relacionados: si $a \neq b$, $(a, b) \notin Id_A$ y $(b, a) \notin Id_A$.

Ejemplo 4.6 $R = (A \times A) \setminus Id_A$ es la *relación diferencia* en A.

Ejemplo 4.7 La *relación inclusión* en $\mathcal{P}(X)$ es

$$\{(A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) : A \subseteq B\}.$$

A partir de ahora escribiremos xRy para denotar $(x, y) \in R$.

Definición 4.8 (a) Decimos que x *está en relación* R *con* y si xRy.

(b) El conjunto de todos los x que están en relación R con algún y es llamado *dominio* de R y es denotado por $dom\, R$.

(c) El conjunto de todos los y tales que para algún x, x está en relación R con y, es llamado *rango* de R y denotado por $ran\, R$.

(d) El conjunto $dom\, R \cup ran\, R$ es llamado *campo* de R y denotado por $cam\ R$.

El dominio y el rango de una relación R también pueden ser descritos como $dom\, R = \{x : \exists\, y \text{ tal que } xRy\}$ (o sea, $dom\, R$ es el conjunto de primeras coordenadas de todos los elementos en R) y $ran\, R = \{y : \exists\, x \text{ tal que } xRy\}$ (o sea, $ran\, R$ es el conjunto de las segundas coordenadas de elementos en R). También obsérvese que si $cam\ R \subseteq X$ podemos entonces decir que R es una relación en X.

Ejemplo 4.9 En el Ejemplo 4.2, $dom\, R = \mathbf{Z}^+$, $ran\, R = \mathbf{Z}$ *y* $cam\ R = dom\, R \cup ran\, R = \mathbf{Z}$.

Ejemplo 4.10 Si R es la relación identidad o la relación diferencia en A, entonces $dom\ R = A = ran\ R$, a menos que A sea unitario, en cuyo caso la relación diferencia es $\emptyset$.

Ejemplo 4.11 $dom\,(A \times B) = A$, $ran\,(A \times B) = B$ y $cam\ (A \times B) = A \cup B$.

Definición 4.12 (a) La *imagen* de un conjunto A bajo R es el conjunto de todos los elementos y del rango de R en relación R con algún elemento de A. Este conjunto es usualmente denotado por $R(A)$. Así,

$$R(A) = \{y \in ran\, R : \exists\, x \in A \ tal\ que\ xRy\}.$$

(b) La *imagen inversa* de un conjunto B bajo R es el conjunto de todos los elementos x del dominio de R en relación R con algún elemento de B. Este conjunto es usualmente denotado por $R^{-1}(B)$. Así,

$$R^{-1}(B) = \{x \in dom\, R : \exists\, y \in B \ tal\ que\ xRy\}.$$

Ejemplo 4.13 Sea R como en 4.2, entonces $R(\{2\})$ es el conjunto de todos los enteros pares (positivos y negativos).

$$R^{-1}(\{-9,-3,8,9,12\}) = \{1,2,3,4,6,8,9,12\}\,.$$

Definición 4.14 Sea R una relación. La *relación inversa de* R es el conjunto:

$$R^{-1} = \{z : z = (x,y) \quad \wedge \quad (y,x) \in R\}$$

De la propia definición de relación inversa se sigue inmediatamente que $(x,y) \in R^{-1}$ si y sólo si $(y,x) \in R$. Esto justifica el nombre de relación inversa para R^{-1}, pues intuitivamente R^{-1} hace lo contrario que R.

Ejemplo 4.15 Consideremos nuevamente la relación

$$R = \left\{(m,n) : m \in \mathbf{Z}^+, n \in \mathbf{Z} \text{ y } m \text{ divide a } n\right\}.$$

Para tal relación,

$$\begin{aligned} R^{-1} &= \{w : w = (n,m) \quad \wedge \quad (m,n) \in R\} \\ &= \{(n,m) : m \text{ entero positivo, } n \text{ entero y } (m,n) \in R\} \\ &= \{(n,m) : n \text{ entero, } m\text{entero positivo y } n \text{ es múltiplo de } m\}\,. \end{aligned}$$

Ejemplo 4.16 $(A \times B)^{-1} = B \times A$.

Ejemplo 4.17 $\emptyset^{-1} = \emptyset$.

Ejemplo 4.18 $(Id_A)^{-1} = Id_A$.

El lector (esperando que el conjunto de lectores sea no vacío) notará que el símbolo $R^{-1}(B)$ usado en la Definición 4.12(b) para la imagen inversa de B bajo R, ahora también es usado para denotar la imagen de B bajo R^{-1}. Afortunadamente estos conjuntos son iguales.

Teorema 4.19 *La imagen inversa de B bajo R es igual a la imagen de B bajo R^{-1}.*

Demostración:

Primero note que el rango de R es igual al dominio de R^{-1}. Ahora $x \in R^{-1}(B)$ si y sólo si existe $y \in B$ tal que $(x,y) \in R$ si y sólo si $(y,x) \in R^{-1}$. Por lo tanto, $x \in R^{-1}(B)$ bajo R si y sólo si para algún y en B, $(y,x) \in R^{-1}$, es decir, si y sólo si x pertenece a la imagen de B bajo R^{-1}. ■

Para simplificar notación, introducimos la siguiente convención. En lugar de escribir

$$\{w : w = (x, y), \text{ para } x, y \text{ con } \mathbf{P}(x, y)\},$$

escribiremos simplemente $\{(x, y) : \mathbf{P}(x, y)\}$. Por ejemplo, dada una relación R, la relación inversa de R puede ser escrita con esta notación como

$$\{(x, y) : (y, x) \in R\}.$$

Obsérvese que, como en el caso general, esta notación es admisible sólo si probamos que existe un conjunto A tal que para todo x, y, $\mathbf{P}(x, y)$ implica que $(x, y) \in A$.

Definición 4.20 Sean R y S relaciones. La *composición de R y S* es la relación

$$S \circ R = \{(x, z) : \exists\, y \text{ para el cual } (x, y) \in R \text{ y } (y, z) \in S\}.$$

Que un par (x, z) pertenezca a $S \circ R$, significa que para algún y, xRy y ySz. Así que para encontrar objetos relacionados con x en $S \circ R$, primero se encuentran objetos y relacionados a x en R y luego objetos z relacionados en S con alguno de los objetos y; todos estos objetos están relacionados en $S \circ R$ con x. Note que de aquí $S \circ R$ no es lo mismo que $R \circ S$ (ver Ejemplo 4.22).

Ejemplo 4.21 Para cualquier relación R, $\emptyset \circ R = \emptyset = R \circ \emptyset$.

Ejemplo 4.22 Si $R = \{(1, 2)\}$ y $S = \{(2, 0)\}$, entonces $S \circ R = \{(1, 0)\}$; mientras que $R \circ S$ es la relación vacía.

Ejemplo 4.23 Si R es una relación en A, entonces $R \circ Id_A = R = Id_A \circ R$.

Ejemplo 4.24 Si $ran\, R \cap dom\, S = \emptyset$, entonces $S \circ R$ es la relación vacía.

Muchas relaciones son de particular interés, aquí introduciremos una muy importante y en el resto del capítulo definiremos algunas otras.

Definición 4.25 La *relación de pertenencia en (o restringida a) A* es definida por

$$\in_A = \{(a, b) : a \in A,\ b \in A \text{ y } a \in b\}.$$

También pueden definirse relaciones ternarias. Más explícitamente, S es una relación ternaria si para cualquier $u \in S$, existen x, y, z tales que $u = (x, y, z)$. Si $S \subseteq A^3$, se dice que S es una relación ternaria en A. Muchos de los conceptos de esta sección pueden ser generalizados a relaciones ternarias.

Ejercicios 4.1

1. Sea R una relación (binaria). Demuestre que $dom\ R \subseteq \bigcup(\bigcup R)$ y que $ran\ R \subseteq \bigcup(\bigcup R)$. Concluya de esto que $dom\ R$ y $ran\ R$ existen.

2. Muestre que R^{-1} y $S \circ R$ existen. (Sugerencia:

$$R^{-1} \subseteq (ranR) \times (domR), S \circ R \subseteq (domR \times ranS).)$$

3. Sean R una relación y A, B conjuntos. Pruebe:

   (a) $R(A \cup B) = R(A) \cup R(B)$.
   (b) $R(A \cap B) \subseteq R(A) \cap R(B)$.
   (c) $R(A \setminus B) \supseteq R(A) \setminus R(B)$.
   (d) Por medio de ejemplos muestre que $\subseteq$ y $\supseteq$ en (b) y (c) no pueden reemplazarse por $=$.
   (e) Pruebe los incisos (a), ..., (d) con R^{-1} en vez de R.

4. Sean $\mathcal{A}$ una familia de conjuntos y R una relación. Muestre que:

   (a) $R(\bigcup \mathcal{A}) = \bigcup \{R(A) : A \in \mathcal{A}\}$.
   (b) $R(\bigcap \mathcal{A}) \subseteq \bigcap \{R(A) : A \in \mathcal{A}\}$.

5. Sea $R \subseteq X \times Y$. Demuestre:

   (a) $R(X) = ran\ R$ y $R^{-1}(Y) = dom\ R$.
   (b) Si $a \notin dom\ R$, $R(\{a\}) = \emptyset$; si $b \notin ran\ R$, $R^{-1}(\{b\}) = \emptyset$.
   (c) $dom\ R = ran\ R^{-1}$; $ran\ R = dom\ R^{-1}$.
   (d) $(R^{-1})^{-1} = R$.
   (e) $R^{-1} \circ R \supseteq Id_{dom\,R}$, $R \circ R^{-1} \supseteq Id_{ran\,R}$. Dar un ejemplo de una relación R tal que $R^{-1} \circ R \neq Id_{dom\,R}$ y $R \circ R^{-1} \neq Id_{ran\,R}$.

6. Verifique el Ejemplo 4.24.

7. Pruebe que para tres relaciones R, S y T

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

   (La operación $\circ$ es asociativa.)

8. Sean $X = \{\emptyset, \{\emptyset\}\}$ y $Y = \mathcal{P}(X)$. Describa:

   (a) $\in_Y$.

   (b) Id_Y.

   (c) Determine el dominio, rango y campo de ambas relaciones.

9. Muestre que si $\mathcal{M}$ es una familia no vacía de relaciones entonces $\bigcap \mathcal{M}$ es una relación.

4.2 Funciones

La palabra *función* fue introducida a las matemáticas por Leibniz, quien originalmente utilizó este término para referirse a cierta clase de fórmulas matemáticas. La idea de Leibniz estaba muy limitada, y el significado de la palabra tuvo desde entonces muchas fases de generalización. Hoy en día, el significado de función es esencialmente el siguiente: Dados dos conjuntos A y B, una función de A en B es una correspondencia que asocia con cada elemento de A un único elemento de B. Una función, por tanto, representa un tipo especial de relación: una relación donde todo objeto del dominio está relacionado precisamente con un único objeto del rango, nombrado el valor de la función.

Definición 4.26 Una relación f es llamada *función* si $(a, b) \in f$ y $(a, c) \in f$ implica que $b = c$ para cualesquiera a, b, c.[1]

En otras palabras, una relación f es una función si y sólo si para todo $a \in dom\ f$ hay exactamente un b tal que $(a, b) \in f$. Este único b es llamado *valor de f en a* y es usualmente denotado por $f(a)$; aunque en algunas ocasiones es muy conveniente la notación f_a. Si f es una función con $dom\, f = A$ y $ran\, f \subseteq B$, entonces

$$f = \{(a, f(a)) : a \in A\}$$

y es costumbre emplear la notación $f : A \to B$ para denotar la función f; o de manera más precisa:

$$\begin{array}{rll} f: & A & \longrightarrow B \\ & a & \mapsto f(a) \end{array}$$

Obsérvese que si $a \notin A$, $f(a)$ carece de sentido.

[1] Esta definición de función fue propuesta por G. Peano [P_2].

Ejemplo 4.27 Si $A = \{1, 2, 3\}$ y $B = \{1, 2\}$, entonces

$$f = \{(1, 1), (1, 2), (2, 2), (3, 1)\}$$

no es una función ya que $(1, 1)$ y $(1, 2)$ pertenecen a f, y sin embargo $1 \neq 2$.

Ejemplo 4.28 Sean X y Y son conjuntos y sea $b \in Y$. Entonces $f = X \times \{b\}$ es una función, llamada *función constante* de X en Y.

Ejemplo 4.29 Si X es un conjunto, $f = \left\{(x, y) \in X^2 : x = y\right\}$ es función, se llama *identidad* en X, $f = Id_X$. Ver Ejemplo 4.5.

Ejemplo 4.30 Sean X un conjunto y A un subconjunto de X. Definamos $\chi_A \colon X \to \{0, 1\}$ por la regla

$$\chi_A(x) = \begin{cases} 1, & si\ x \in A \\ 0, & si\ x \notin A \end{cases}$$

para cada $x \in X$. Esta importante función se llama la *función característica* de A.

Ejemplo 4.31 Sean X un conjunto y $A \subseteq X$. La función $i_A = \{(x, x) : x \in A\}$ es llamada *inclusión de A en X* y usualmente se denotada por $i_A : A \hookrightarrow X$.

Ejemplo 4.32 Si A y B son conjuntos, entonces tenemos dos funciones naturales: $p_1 : A \times B \to A$ y $p_2 : A \times B \to B$ tales que $p_1(a, b) = a$ y $p_2(a, b) = b$. Se llaman *proyecciones en la primera* y *la segunda coordenada*, respectivamente.

Ejemplo 4.33 Sea X un conjunto $f : \mathcal{P}(X) \to \mathcal{P}(X)$ definida como $f(A) = X \setminus A$ es una función.

Puesto que las funciones son relaciones, los conceptos de rango, imagen, inversa y composición pueden ser aplicados. Si $f : A \to B$ y $A_1 \subseteq A$, $B_1 \subseteq B$ tenemos que $f \subseteq A \times B$, la imagen de A_1 bajo f es el conjunto

$$\begin{aligned} f(A_1) &= \{y \in B : (x, y) \in f,\ x \in A_1\} \\ &= \{f(x) : x \in A_1\}. \end{aligned}$$

La imagen inversa bajo f de B_1 es

$$\begin{aligned} f^{-1}(B_1) &= \{x \in A : (x, y) \in f,\ \text{para algún } y \in B_1\} \\ &= \{x \in A : f(x) \in B_1\}. \end{aligned}$$

Obsérvese que la descripción de estos conjuntos es más simple para funciones que para relaciones en general (ver Definición 4.12).

Teorema 4.34 *Supongamos que $f : X \to Y$ es una función, entonces:*

(a) Para $A \subseteq X$ resulta que $A = \emptyset$ si y sólo si $f(A) = \emptyset$.

(b) $f^{-1}(\emptyset) = \emptyset$.

(c) $f(\{x\}) = \{f(x)\}$.

(d) Si $A \subseteq B \subseteq X$ entonces

$$f(A) \subseteq f(B) \quad y \quad f(B \setminus A) \supseteq f(B) \setminus f(A).$$

(e) Si $A' \subseteq B' \subseteq Y$ entonces

$$f^{-1}(A') \subseteq f^{-1}(B') \quad y \quad f^{-1}(B' \setminus A') = f^{-1}(B') \setminus f^{-1}(A').$$

(f) Si $\{A_\alpha\}_{\alpha \in I}$ es una familia indizada de subconjuntos de X y $\{A'_\alpha\}_{\alpha \in I}$ es una familia indizada de subconjuntos de Y, entonces

$$f\left(\bigcup_{\alpha \in I} A_\alpha\right) = \bigcup_{\alpha \in I} f(A_\alpha) \quad , \quad f\left(\bigcap_{\alpha \in I} A_\alpha\right) \subseteq \bigcap_{\alpha \in I} f(A_\alpha)$$

$$f^{-1}\left(\bigcup_{\alpha \in I} A_\alpha\right) = \bigcup_{\alpha \in I} f^{-1}(A_\alpha) \quad , \quad f^{-1}\left(\bigcap_{\alpha \in I} A_\alpha\right) = \bigcap_{\alpha \in I} f^{-1}(A_\alpha)$$

(g) Si $A \subseteq X$ es tal que $A \subseteq f^{-1}(f(A))$, y si $A' \subseteq Y$,

$$f(f^{-1}(A')) = A' \cap f(X).$$

Demostración:

(a) Esto se obtiene ya que f es una función (para todo $x \in X$, existe $y \in Y$ tal que $(x, y) \in f$) y por la definición de $f(A) = \{f(x) : x \in A\}$.

(b) Es clara.

(c) Esto se debe a que $(x, y_1) \in f$ y $(x, y_2) \in f$ implica $y_1 = y_2$.

(d) Veamos primero que $f(A) \subseteq f(B)$. Si $y \in f(A)$ entonces existe $x \in A$ tal que $f(x) = y$. Como $A \subseteq B$ entonces $x \in B$, luego $y \in f(B)$. Por lo tanto, $f(A) \subseteq f(B)$.

Si $y \in f(B) \setminus f(A)$ entonces $y \in f(B)$ y $y \notin f(A)$, por lo que se deduce la existencia de $x \in B$ tal que $f(x) = y$. Además, como $y \notin f(A)$, entonces para cualquier $a \in A$, $f(a) \neq y$, con lo cual $x \in B \setminus A$; así, $y \in f(B \setminus A)$. Por lo tanto, $f(B) \setminus f(A) \subseteq f(B \setminus A)$.

(e) Veamos primero que $f^{-1}(A') \subseteq f^{-1}(B')$, si $A' \subseteq B'$. Si $x \in f^{-1}(A')$ entonces existe $y \in A'$ tal que $f(x) = y$. Como $A' \subseteq B'$ y $y \in B'$, $x \in f^{-1}(B')$. Por lo tanto, $f^{-1}(A') \subseteq f^{-1}(B')$. Ahora veamos que $f^{-1}(B' \setminus A') = f^{-1}(B') \setminus$

$f^{-1}(A')$. En efecto, $x \in f^{-1}(B' \setminus A')$ si y sólo si existe $y \in B'$ y $y \notin A'$ tal que $f(x) = y$ si y sólo si $x \in f^{-1}(B') \setminus f^{-1}(A')$.

(f) Demostraremos únicamente que

$$f\left(\bigcup_{\alpha\in I} A_\alpha\right) = \bigcup_{\alpha\in I} f(A_\alpha),$$

dejando como ejercicio las igualdades restantes.

$y \in f\left(\bigcup_{\alpha\in I} A_\alpha\right)$ si y sólo si existe $x \in \bigcup_{\alpha\in I} A_\alpha$ con $f(x) = y$ si y sólo si existen $\alpha \in I$ y $x \in A_\alpha$ tales que $f(x) = y$ si y sólo si existe $\alpha \in I$ tal que $y \in f(A_\alpha)$ si y sólo si $y \in \bigcup_{\alpha\in I} f(A_\alpha)$. Por lo tanto, $f\left(\bigcup_{\alpha\in I} A_\alpha\right) = \bigcup_{\alpha\in I} f(A_\alpha)$.

(g) Ejercicio. ■

El Axioma de Extensión puede ser aplicado a funciones como sigue:

Lema 4.35 *Sean f y g funciones. $f = g$ si y sólo si $dom\, f = dom\, g$ y $f(x) = g(x)$ para todo $x \in dom\, f$.*

Demostración:

$\Rightarrow$] Demostraremos primero que $f = g$ implica $dom\, f = dom\, g$. $x \in dom\, f$ si y sólo si existe algún y para el cual $(x, y) \in f$ si y sólo si existe algún y para el cual $(x, y) \in g$ (pues el conjunto f es igual al conjunto g) si y sólo si $x \in dom\, g$.

Por otra parte si existe $x \in dom\, f$ tal que $f(x) \neq g(x)$ entonces $(x, f(x)) \in f$ y $(x, f(x)) \notin g$ (pues g es función), entonces $(x, f(x)) \in f \setminus g$, es decir, $f \neq g$.

$\Leftarrow$] Supongamos que $dom\, f = dom\, g$ y que para cada $x \in dom\, f$, $f(x) = g(x)$. $(x, y) \in f$ si y sólo si $x \in dom\, f$ y $f(x) = y$ si y sólo si $x \in dom\, g$ y $g(x) = y$ si y sólo si $(x, y) \in g$. Por lo tanto, $f = g$. ■

Introducimos también otras definiciones.

Definición 4.36 Sea f una función y A, B conjuntos:

(a) *f es una función desde A* si *$dom\ f \subseteq A$.*

(b) *f es una función en A* si *$dom\, f = A$.*

(c) *f es una función hacia B* si *$ran\, f \subseteq B$.*

(d) La *restricción de la función f a A* es la función

$$f\,|_A = \{(a, b) \in f : a \in A\}.$$

Si g es una restricción de f para algún A, decimos que f es una *extensión* de g.

Es costumbre emplear la frase: f es una función de A en B, cuando f es una función en A y f es una función hacia B; o sea, $f : A \to B$.

Ejemplo 4.37 Para cualquier conjunto A, hay una única función f de $\emptyset$ en A, a saber, la función vacía, $f = \emptyset$.

Ejemplo 4.38 Sea $f = \left\{(x, \frac{1}{x^2}) : x \in \mathbf{R} \setminus \{0\}\right\}$. f es una función. En efecto, si $(a, b) \in f$ y $(a, c) \in f$, entonces $b = \frac{1}{a^2}$ y $c = \frac{1}{a^2}$; así, $b = c$. La notación usual para esta función es $f(x) = \frac{1}{x^2}$. f es una función desde el conjunto de los números reales, pero no en el conjunto de los números reales pues $0 \notin dom\, f$. Esta es una función en $A = \mathbf{R}\setminus\{0\} = dom\, f$ y hacia el conjunto de los números reales. Si $C = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$, entonces $f(C) = \{x \in \mathbf{R} : x \geq 1\}$ y $f^{-1}(C) = \{x \in \mathbf{R} : x \leq -1 \ \vee \ x \geq 1\}$. La composición $f \circ f$ es la relación:

$$\begin{aligned} f \circ f &= \{(x, z) : \exists\, y \text{ para el cual } (x, y) \in f,\ (y, z) \in f\} \\ &= \left\{(x, z) : \exists\, y \text{ para el cual } x \neq 0,\ y = \tfrac{1}{x^2},\ z = \tfrac{1}{y^2}\right\} \\ &= \left\{(x, z) : x \neq 0,\ z = x^4\right\}; \end{aligned}$$

así, $f \circ f(x) = x^4$. Note que $f \circ f$ es una función; esto no es un accidente.

Teorema 4.39 *Sean f y g funciones. Entonces $g \circ f$ es una función. $g \circ f$ está definida en x si y sólo si f está definida en x y g está definida en $f(x)$, es decir, $dom\, g \circ f = dom\ f \cap f^{-1}(dom\ g)$.*

Demostración:

Se mostrará que $g \circ f$ es una función. Si $(x, z_1) \in g \circ f$ y $(x, z_2) \in g \circ f$ entonces existen y_1, y_2 tales que $(x, y_1) \in f$ y $(y_1, z_1) \in g$, $(x, y_2) \in f$ y $(y_2, z_2) \in g$. Puesto que f es una función, $y_1 = y_2$. Así tenemos que $(y_1, z_1) \in g$ y $(y_1, z_2) \in g$. Entonces $z_1 = z_2$, porque también g es una función.

Por otra parte, $x \in dom\ g \circ f$ si y sólo si existe algún z tal que $(x, z) \in g \circ f$, es decir, hay un y tal que $(x, y) \in f$ y $(y, z) \in g$. Lo anterior se satisface si y sólo si:

$$x \in dom\, f \quad \text{y} \quad y = f(x) \in dom\, g,$$

o sea, $x \in dom\, f$ y $x \in f^{-1}(dom\, g)$. ■

Se desprende inmediatamente el siguiente resultado.

Corolario 4.40 *Si $ran\, f \subseteq dom\, g$, entonces $dom\, g \circ f = dom\, f$.*

Es importante señalar que la composición de funciones siempre está definida, de hecho, si $ran\, f \cap dom\, g = \emptyset$, la composición de f con g es la función vacía,

$g \circ f = \emptyset$. Pero $\emptyset$ es una función de poco interés, por lo cual generalmente se restringe la composición al caso en que $ran\, f \subseteq dom\, g$, por ser el caso verdaderamente interesante. Pero no hay alguna razón para no definir la composición de cualquier par de funciones.

Veamos un ejemplo típico del uso del teorema anterior para encontrar la composición de funciones.

Ejemplo 4.41 Encontrar la composición y el dominio de la composición de las siguientes funciones:

$$f = \left\{(x, x^2 - 1) : x \in \mathbf{R}\right\}, \quad g = \left\{(x, \sqrt{x}) : x \in \mathbf{R},\ x \geq 0\right\}.$$

Determinaremos primero el dominio de $g \circ f$. $dom\, f$ es el conjunto de todos los números reales y $dom\, g = \{x \in \mathbf{R} : x \geq 0\}$. Entonces

$$\begin{aligned} f^{-1}(dom\, g) &= \{x \in \mathbf{R} : f(x) \in dom\, g\} \\ &= \left\{x : x^2 - 1 \geq 0\right\} \\ &= \{x \in \mathbf{R} : x \geq 1 \ \vee \ x \leq -1\}. \end{aligned}$$

Por lo tanto,

$$dom\, g \circ f = dom\, f \cap f^{-1}(dom\, g) = \{x \in \mathbf{R} : x \geq 1 \ \vee \ x \leq -1\}$$

y

$$\begin{aligned} g \circ f &= \left\{(x, z) : x^2 - 1 \geq 0 \ \wedge \ \exists y \in \mathbf{R},\ y = x^2 - 1 \ \wedge \ z = \sqrt{y}\right\} \\ &= \left\{\left(x, \sqrt{x^2 - 1} : x \geq 1 \ \vee \ x \leq -1\right\}\right. . \end{aligned}$$

Ahora derivemos algunas propiedades de la composición de funciones.

Teorema 4.42 *Sean $f : A \to B$, $g : B \to C$ y $h : C \to D$ funciones.*

(a) Si $A' \subseteq A$, entonces $g \circ f(A') = g(f(A'))$.

(b) Si $C' \subseteq C$, entonces $(g \circ f)^{-1}(C') = f^{-1}(g^{-1}(C'))$.

(c) $h \circ (g \circ f) = (h \circ g) \circ f$, es decir, la composición de funciones es asociativa.

Demostración:

Se dejan como ejercicio las partes *(a)* y *(b)*. Pasaremos a demostrar la parte *(c)*.

$(x, z) \in h \circ (g \circ f)$ si y sólo si existe w tal que $(x, w) \in g \circ f$ y $(w, z) \in h$ si y sólo si existe y tal que $(x, y) \in f$, $(y, w) \in g$ y $(w, z) \in h$ si y sólo si $(x, y) \in f$

y $(y,z) \in h \circ g$ si y sólo si $(x,z) \in (h \circ g) \circ f$. ■

Si f es una función, f^{-1} es una relación, pero no necesariamente una función. Decimos que una función f es *invertible*, si f^{-1} es una función, es decir, la relación

$$f^{-1} = \{(y,x) : (x,y) \in f\},$$

es una función.

Es importante encontrar condiciones necesarias y suficientes para que una función sea invertible.

Definición 4.43 Una función f es llamada *inyectiva* (o *uno a uno*) si $a_1 \in dom\, f$, $a_2 \in dom\, f$ y $a_1 \neq a_2$ implica $f(a_1) \neq f(a_2)$.

La definición anterior se puede expresar en otras palabras diciendo que: $a_1 \in dom\, f$, $a_2 \in dom\, f$ y $f(a_1) = f(a_2)$ implica $a_1 = a_2$. Así, una función inyectiva asigna diferentes valores para diferentes elementos de su dominio.

Teorema 4.44 *Una función es invertible si y sólo si es inyectiva.*

Demostración:

$\Rightarrow$] Sea f una función invertible entonces f^{-1} es una función. Si $a_1 \in dom\, f$, $a_2 \in dom\, f$, y $f(a_1) = f(a_2)$, entonces tenemos que $(f(a_1), a_1) \in f^{-1}$ y $(f(a_2), a_2) \in f^{-1}$, lo cual implica que $a_1 = a_2$. Así, f es inyectiva.

$\Leftarrow$] Sea f una función inyectiva. Si $(a, b_1) \in f^{-1}$ y $(a, b_2) \in f^{-1}$, tenemos que $(b_1, a) \in f$ y $(b_2, a) \in f$. Por lo tanto, $b_1 = b_2$, y así hemos probado que f^{-1} es función. ■

Si consideramos la función $f : X \to \mathbf{R}$, donde $X = \{x \in \mathbf{R} : x \geq 0\}$ y $f(x) = x^2$, podemos demostrar que dicha función es inyectiva, por lo cual f es una función invertible. Pero el dominio de f^{-1} es $\{x \in \mathbf{R} : x \geq 0\}$. De modo que a f^{-1} no la podemos considerar como una función de $\mathbf{R}$ en X tal que $f^{-1} \circ f = Id_X$ y $f \circ f^{-1} = Id_{\mathbf{R}}$. Estamos interesados en hallar una función $g^{-1} : B \to A$ que actúe inversamente con respecto a $g : A \to B$ cuando sea posible; o sea, $g^{-1} \circ g = Id_A$ y $g \circ g^{-1} = Id_B$. Si observamos, el problema de la función $f : X \to \mathbf{R}$ es que su rango no es todo $\mathbf{R}$.

Definición 4.45 Sea $f : A \to B$ una función:

(a) f se llama *sobreyectiva* si $f(A) = B$.

(b) f se llama *biyectiva* si es inyectiva y sobreyectiva.

Notemos que una función $f : A \to B$ es biyectiva si y sólo si para cada $b \in B$, existe un único $a \in A$ tal que $f(a) = b$. Este $a \in A$ existe por la sobreyectividad de f, y es único por la inyectividad de f.

Ahora, si $f : A \to B$ es una función biyectiva entonces $dom\, f^{-1} = B$, es decir, se puede definir

$$f^{-1} : B \to A$$

por la regla: $f^{-1}(b)$ es el único $a \in A$ tal que $f(a) = b$. Además, con esto último tenemos que f^{-1} cumple las relaciones:

$$f^{-1} \circ f = Id_A \quad \text{y} \quad f \circ f^{-1} = Id_B,$$

las cuales expresan precisamente que f^{-1} actúa de manera inversa a como lo hace f sobre todo el conjunto A y que f actúa de manera inversa a como lo hace f^{-1} sobre todo el conjunto B. En el Teorema 4.52(c), mostraremos que f^{-1} es única, lo cual nos permite hacer la definición 4.47; antes un útil ejemplo.

Ejemplo 4.46 Para cualquier conjunto A, la función identidad es una biyección en A. Obsérvese que en caso de que $A = \emptyset$, Id_A es la función vacía y que es biyectiva en este (único) caso.

Definición 4.47 Si $f : A \to B$ es una función biyectiva, a la función $f^{-1} : B \to A$ se le llamará *función inversa de* $f : A \to B$.

Note que a $f^{-1} : B \to A$ se le llama función inversa de $f : A \to B$, y no sólo de f, para recalcar el hecho de que f^{-1} depende de los conjuntos A y B.

En seguida daremos múltiples caracterizaciones del concepto de inyectividad y sobreyectividad.

Teorema 4.48 *Sea $f : X \to Y$ una función con $X \neq \emptyset$. Entonces los siguientes enunciados son equivalentes:*

(a) f es inyectiva.
(b) Para todo $x_1 \in X$, $x_2 \in X$, $f(x_1) = f(x_2)$ implica $x_1 = x_2$.
(c) Existe $g : Y \to X$ tal que $g \circ f = Id_X$.
(d) Para cualesquiera $h, k : Z \to X$, $f \circ h = f \circ k$ implica $h = k$.
(e) Para todo $A \subseteq X$, $f^{-1}(f(A)) = A$.
(f) Para cualesquiera $A \subseteq B \subseteq X$, $f(B \setminus A) = f(B) \setminus f(A)$.
(g) Para cualesquiera $A \subseteq X$, $B \subseteq X$, $f(A \cap B) = f(A) \cap f(B)$.

DEMOSTRACIÓN:

(a) $\Rightarrow$ *(b)* Obvio.

(b) $\Rightarrow$ *(c)* Sea $x_0 \in X$ y definamos $g : Y \to X$ del siguiente modo:

$$g(y) = \begin{cases} x_0, & \text{si } y \notin f(X) \\ x, & \text{si } y = f(x). \end{cases}$$

g es claramente una función, pues si $(y, x_1) \in g$ y $(y, x_2) \in g$ tenemos dos posibilidades: si $y \notin f(X)$, por definición $x_1 = x_2 = x_0$. Si $y \in f(X)$ entonces $f(x_1) = f(x_2)$ y por *(b)* $x_1 = x_2$.

Luego, para $x \in X$, $g \circ f(x) = g(f(x)) = x$; con lo cual, $g \circ f = Id_X$.

(c) $\Rightarrow$ *(d)* Si $h, k : Z \to X$ son funciones tales que $f \circ h = f \circ k$, entonces por hipótesis existe una función $g : Y \to X$ tal que $g \circ f = Id_X$, con lo cual: $h = Id_X \circ h = (g \circ f) \circ h = g \circ (f \circ h) = g \circ (f \circ k) = (g \circ f) \circ k = Id_X \circ k = k$.

(d) $\Rightarrow$ *(e)* Sea $A \subseteq X$. Sabemos que $A \subseteq f^{-1}(f(A))$ para cualquier función (Teorema 4.34(g)). Ahora bien, si $x \in f^{-1}(f(A))$ entonces $f(x) \in A$, luego existe $a \in A$ tal que $f(a) = f(x)$.

Sean $h, k : \{1\} \to X$ definidas como $h(1) = a$ y $k(1) = x$, entonces $f \circ h = f \circ k$. Por hipótesis $h = k$, y así $a = x$; con esto concluimos que $A \supseteq f^{-1}(f(A))$.

(e) $\Rightarrow$ *(f)* Sean A y B dos conjuntos tales que $A \subseteq B \subseteq X$ y supongamos que $f(x) \in f(B \setminus A)$ con $x \in B \setminus A$. Entonces $f(x) \in f(B)$; pero como $x \notin A$ y $A = f^{-1}(f(A))$, entonces $x \notin f^{-1}(f(A)$. Esto implica que $f(x) \notin f(A)$; así, $f(x) \in f(B) \setminus f(A)$. Como siempre ocurre $f(B) \setminus f(A) \subseteq f(B \setminus A)$, concluimos entonces que $f(B) \setminus f(A) = f(B \setminus A)$.

(f) $\Rightarrow$ *(g)* Sean $A \subseteq X$ y $B \subseteq X$. Se sabe que $f(A \cap B) \subseteq f(A) \cap f(B)$. Si $y \in f(A) \cap f(B)$, entonces $y = f(x)$ con $x \in A$. Si ocurriera $x \notin B$, entonces $x \in X \setminus B$. Por lo cual, $f(x) \in f(X \setminus B) = f(X) \setminus f(B)$, y así, $y = f(x) \notin f(B)$ que es una contradicción. Por lo tanto, $f(x) \in f(B)$ implica $x \in B$, y así $x \in A \cap B$. Por todo lo anterior, $y \in f(A \cap B)$.

(g) $\Rightarrow$ *(a)* Trivial. ■

Teorema 4.49 *Si $f : X \to Y$ es una función entonces, son equivalentes:*

(a) f es sobreyectiva.

(b) Para todo $y \in Y$, existe $x \in X$ tal que $f(x) = y$.

(c) Para todo subconjunto no vacío A de Y, $f^{-1}(A) \neq \emptyset$.

(d) Para todo subconjunto B de Y, $B = f(f^{-1}(B))$.

(e) Para cualesquiera $h, k : Y \to Z$, $h \circ f = k \circ f$ implica $h = k$.

DEMOSTRACIÓN:

Las implicaciones *(a)* $\Rightarrow$ *(b)* y *(b)* $\Rightarrow$ *(c)* son obvias.

(c) $\Rightarrow$ *(d)* Sabemos que $f(f^{-1}(B)) = f(X) \cap B \subseteq B$. Si la contención fuese estricta, entonces $A = B \setminus f(f^{-1}(B)) \neq \emptyset$, lo que implica $f^{-1}(A) \neq \emptyset$; con lo cual se deduce que existe un $x \in X$ tal que

$$f(x) \in B \setminus f(f^{-1}(B));$$

pero esto es imposible.

(d) $\Rightarrow$ *(e)* Sean $h, k : Y \to Z$ dos funciones cualesquiera tales que $h \circ f = k \circ f$. Sea $y \in Y$. Como $f(f^{-1}(\{y\})) = \{y\}$, por el Teorema 4.34(a), $f^{-1}(\{y\}) \neq \emptyset$. Sea $x \in X$ tal que $x \in f^{-1}(\{y\})$; o sea, $f(x) = y$. Tenemos entonces que $h(y) = h(f(x)) = h \circ f(x) = k \circ f(x) = k(f(x)) = k(y)$. Por el Lema 4.35, se sigue que $h = k$.

(e) $\Rightarrow$ *(a)* Si $f : X \to Y$ no es sobreyectiva, defina funciones $h, k : Y \to \{1, 2\}$ por $h = Y \times \{1\}$ y

$$k(y) = \begin{cases} 1, & \text{si } y \in f(X) \\ 2, & \text{si } y \notin f(X). \end{cases}$$

Entonces, $h \circ f = k \circ f$, pero $h \neq k$. ■

La parte (d) del Teorema 4.48 motiva la siguiente definición.

Definición 4.50 Sea $f : X \to Y$ una función.

(a) *A* una función $g : Y \to X$ tal que $g \circ f = Id_X$ *se* le llama *inversa izquierda de* $f : X \to Y$.

(b) *A* una función $h : Y \to X$ tal que $f \circ h = Id_Y$ se le llama *inversa derecha de* $f : X \to Y$.

Es factible pensar que, así como las funciones inyectivas se caracterizan por tener inversa izquierda, las funciones sobreyectivas se caractericen por tener inversa derecha; esta conjetura es correcta, no obstante, en un capítulo posterior veremos que esta proposición es equivalente a uno de los Axiomas de la Teoría de Conjuntos (el Axioma de Elección), por lo cual no es trivial (aunque sí fácil de establecer a partir de ese axioma). Lo que sí es posible demostrar ahora es la siguiente proposición.

Proposición 4.51 *Si* $f : X \to Y$ *tiene una inversa derecha* $g : Y \to X$, *entonces* f *es sobreyectiva.*

Demostración:

Para cualquier $y \in Y$, poniendo $x = g(y)$, se tiene que $f(x) = y$. Por lo tanto, f es sobreyectiva. ■

Teorema 4.52 *Sean $f : X \to Y$ y $g : Y \to Z$ dos funciones. Entonces:*

(a) La inyectividad de f y g implica la inyectividad de $g \circ f$.

(b) La sobreyectividad de f y g implica la sobreyectividad de $g \circ f$.

(c) Si $X = Z$, y f y g son tales que

$$g \circ f = Id_X \quad y \quad f \circ g = Id_Y,$$

entonces $g = f^{-1}$, es decir, la inversa de $f : X \to Y$ es única.

DEMOSTRACIÓN:

(a) Sean $A \subseteq X$ y $B \subseteq X$. Entonces haciendo uso de los Teoremas 4.42(a) y 4.48(g), $g \circ f(A \cap B) = g(f(A \cap B)) = g(f(A) \cap f(B)) = g(f(A)) \cap g(f(B)) = g \circ f(A) \cap g \circ f(B)$. Por lo tanto, $g \circ f$ es inyectiva.

(b) Sea $A \subseteq Z$ un subconjunto no vacío, usemos los Teoremas 4.42(b) y 4.49(c). $(g \circ f)^{-1}(A) = f^{-1}(g^{-1}(A))$. Como g es sobreyectiva $g^{-1}(A) \neq \emptyset$, y puesto que f también es sobreyectiva,

$$f^{-1}(g^{-1}(A)) \neq \emptyset.$$

Por lo tanto, $g \circ f$ es sobreyectiva.

(c) Empleando el Teorema 4.48(c) y la Proposición 4.51, obtenemos que f y g también son funciones biyectivas. De aquí se sigue que $dom\, f^{-1} = dom\, g = Y$. Ahora, si $y \in Y$, entonces

$$f(g(y)) = y = f(f^{-1}(y)).$$

Por la inyectividad de f se sigue que $g(x) = f^{-1}(x)$. Concluimos que $g = f^{-1}$, por el Lema 4.35. ■

Una de las razones por las cuales las funciones biyectivas son tan importantes es la que a continuación exponemos. Supongamos que X y Y son dos conjuntos y que $f : X \to Y$ es una función biyectiva entre ellos. Si únicamente estamos interesados en X como conjunto, es decir, sin atender a la naturaleza de sus elementos, entonces podemos considerar a estos dos conjuntos como "*equivalentes*" desde el punto de vista de la Teoría de Conjuntos puesto que cualquier afirmación y construcción de la Teoría de Conjuntos que sea posible realizar con X también se puede realizar con Y. Sólo como una muestra, si Z es otro conjunto y estamos interesados en funciones de X en Z, entonces cualquier función $g : X \to Z$ tiene una única función correspondiente $\widetilde{g} : Y \to Z$, a saber, $\widetilde{g} = g \circ f^{-1}$. Así entonces, podemos "cambiar" nuestro estudio de las funciones de X en Z por el estudio de las funciones de Y en Z. Podríamos dar

otros ejemplos que muestren la paridad de afirmaciones o construcciones que podemos realizar con X y Y; sin embargo, creemos que es más conveniente notar que esta paridad se debe al hecho de que la función f traslada uno a uno tanto a los elementos como a los subconjuntos de X a Y. Por ende, reiteramos que desde el punto de vista de la Teoría de Conjuntos, aunque X y Y sean objetos (posiblemente) distintos, ellos pueden considerarse "equivalentes" ya que son, salvo por "sus nombres", indistinguibles.

Definición 4.53 (a) Las funciones f *y* g son llamadas *compatibles* si $f(x) = g(x)$ para todo $x \in dom\, f \cap dom\, g$.

(b) Un conjunto de funciones $\mathcal{F}$ es llamado *sistema compatible de funciones* si cualesquiera dos funciones $f \in \mathcal{F}$ y $g \in \mathcal{F}$ son compatibles.

Lema 4.54 *(a) Las funciones f y g son compatibles si y sólo si $f \cup g$ es una función.*

(b) Las funciones f y g son compatibles si y sólo si

$$f\,|_{dom\, f \cap dom\, g} = g\,|_{dom\, f \cap dom\, g}\,.$$

Demostración:

(a) $\Rightarrow$] Sean $(x, y) \in f \cup g$ y $(x, z) \in f \cup g$, entonces $x \in dom\, f \cup dom\, g$.

Si $x \in dom\, f \triangle dom\, g$, necesariamente $(x, y) \in f \setminus g$ y $(x, z) \in f \setminus g$. O bien, $(x, y) \in g \setminus f$ y $(x, z) \in g \setminus f$, y en este caso, se concluye que $y = z$.

Si por el contrario $x \in dom\, f \cap dom\, g$, por hipótesis $f(x) = g(x)$; así, $y = f(x) = z$. Por lo tanto, $f \cup g$ es función.

$\Leftarrow$] Sea $x \in dom\, f \cap dom\, g$. Entonces $(x, f(x)) \in f \cup g$ y $(x, g(x)) \in f \cup g$. Como $f \cup g$ es función, se sigue que $f(x) = g(x)$.

(b) Ejercicio. ■

El siguiente teorema nos dice que las funciones en un sistema compatible pueden reunirse en una única función la cual extiende a cada función que es elemento del sistema.

Teorema 4.55 *Si $\mathcal{F}$ es un sistema de funciones compatibles, entonces $\bigcup \mathcal{F}$ es una función con dom $\bigcup \mathcal{F} = \bigcup \{dom\, f : f \in F\}$. Además, la función $\bigcup \mathcal{F}$ extiende a cada $f \in \mathcal{F}$.*

Demostración:

Claramente $\bigcup \mathcal{F}$ es una relación; probaremos que es una función. Si $(a, b) \in \bigcup \mathcal{F}$ y $(a, c) \in \bigcup \mathcal{F}$, hay funciones $f_1, f_2 \in \mathcal{F}$ tales que $(a, b) \in f_1$ y $(a, c) \in f_2$.

Pero f_1 y f_2 son compatibles, y como $(a,b) \in f_1 \cup f_2$, $(a,c) \in f_1 \cup f_2$ y $f_1 \cup f_2$ es una función, entonces $b = c$.

Luego, $x \in dom \bigcup \mathcal{F}$ si y sólo si para algún y, $(x,y) \in \bigcup \mathcal{F}$ si y sólo si $(x,y) \in f$ para alguna $f \in \mathcal{F}$ si y sólo si $x \in dom\, f$ si y sólo si $x \in \bigcup \{dom\, f : f \in F\}$. Por lo tanto, $\bigcup \mathcal{F} = \bigcup \{dom\, f : f \in F\}$. Claramente $\bigcup \mathcal{F}$ extiende a cada $f \in \mathcal{F}$. ■

Para finalizar esta sección tenemos la siguiente definición.

Definición 4.56 Sean A y B conjuntos, el conjunto de todas las funciones de A en B es denotado por B^A.

De hecho, nosotros deberíamos mostrar que tal conjunto existe, pero nos basta observar que $B^A \subseteq \mathcal{P}(A \times B)$.

Ejercicios 4.2

1. Sea $f : X \to Y$ una función. Pruebe que $F : \mathcal{P}(X) \to \mathcal{P}(Y)$ y $G : \mathcal{P}(Y) \to \mathcal{P}(X)$ definidas por:

   $$F(A) = f(A), \qquad G(A) = f^{-1}(A),$$

   son funciones.

2. Completar la demostración del Teorema 4.34.

3. Justifique los procedimientos de los Ejemplos 4.38 y 4.41.

4. Encuentre la función inversa de la función del Ejemplo 4.38.

5. Sean $A \subseteq X$ y sea $f : X \to Y$ una función. Sea $i : A \hookrightarrow X$ la inclusión. Muestre que:

   (a) $f \mid_A = f \circ i$.

   (b) Pongamos $g = f \mid_A$. Entonces $g^{-1}(B) = A \cap f^{-1}(B)$ para cada $B \subseteq Y$.

6. Las funciones f_i, $i = 1, 2, 3, 4$, están definidas como sigue:

$$f_1 = \{(x, 2x-1) : x \in \mathbf{R}\}$$
$$f_2 = \{(x, \sqrt{x}) : x \neq 0\}$$
$$f_3 = \{(x, \sqrt[3]{x}) : x \in \mathbf{R}\}$$
$$f_4 = \left\{(x, \tfrac{1}{x}) : x \in \mathbf{R},\ x \neq 0\right\}$$

   Describa cada una de las siguientes funciones y determine sus dominios y rangos: $f_2 \circ f_1$, $f_1 \circ f_2$, $f_3 \circ f_1$, $f_1 \circ f_3$, $f_4 \circ f_1$, $f_1 \circ f_4$, $f_2 \circ f_4$, $f_4 \circ f_2$, $f_3 \circ f_4$.

7. Sean $f : X \to Y$ y $g : Y \to Z$.

   (a) Si $g \circ f$ es inyectiva, qué se puede decir de la inyectividad de f y de g.

   (b) Si $g \circ f$ es sobreyectiva, qué se puede decir de la sobreyectividad de f y de g.

8. Sean $f : A \to C$ y $g : A \to B$ funciones. Demostrar que existe una función $h : B \to C$ tal que $f = h \circ g$ si y sólo si para cada $x, y \in A$, $g(x) = g(y)$ implica $f(x) = f(y)$.

9. Pruebe la siguiente importante propiedad del producto cartesiano $A \times B$ y de las proyecciones p_1 y p_2. Si $A \neq \emptyset$ y $B \neq \emptyset$, entonces para cualquier conjunto C y cualesquiera funciones $f_1 : C \to A$ y $f_2 : C \to B$ existe una única función $f : C \to A \times B$ tal que $f_1 = p_1 \circ f$ y $f_2 = p_2 \circ f$. Las funciones f_1 y f_2 se llaman las *funciones coordenadas* de f.

10. Sean $f : X \to Y$ y $g : Y \to X$ dos funciones. Demuestre que X y Y pueden expresarse como unión de subconjuntos ajenos, es decir, $X = X_1 \cup X_2$ con $X_1 \cap X_2 = \emptyset$ y $Y = Y_1 \cup Y_2$ con $Y_1 \cap Y_2$, tales que $f(X_1) = Y_1$ y $g(Y_2) = X_2$. (Sugerencia: para cada $A \subseteq X$, sea $Q(A) = X \setminus g(Y \setminus f(A))$. Tómese $X_1 = \bigcap \{Q(A) : Q(A) \subseteq A\}$.)

11. (a) Dar un ejemplo de una función que tenga inversa izquierda pero no inversa derecha.

    (b) Dar un ejemplo de una función que tenga inversa derecha pero no inversa izquierda.

    (c) Dar un ejemplo de una función que tenga dos inversas izquierdas.

    (d) Dar un ejemplo de una función que tenga dos inversas derechas.

(e) Muestre que si $f : X \to Y$ tiene inversa derecha e izquierda entonces es biyectiva.

12. Pruebe que las funciones del Ejercicio 6 son inyectivas.

13. Completar la demostración del Teorema 4.42.

14. Muestre que si $f : A \to B$ y $g : B \to C$ son funciones biyectivas, entonces $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

15. Dar un ejemplo de una función f y un conjunto A, tal que $f \cap A^2 \neq f \mid_A$.

16. Si f es una función inyectiva muestre que

$$f\left(\bigcap_{\alpha\in I} A_\alpha\right) = \bigcap_{\alpha\in I} f(A_\alpha).$$

17. Probar el Lema 4.54(b).

18. Muestre que B^A existe.

19. Pruebe que el conjunto de todas las funciones desde A hacia B es igual a $\bigcup_{X\subseteq A} B^X$.

20. Demuestre la siguiente forma general de distribución:

$$\bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right) = \bigcup_{f\in B^A}\left(\bigcap_{a\in A} F_{a,f(a)}\right),$$

suponiendo que $F_{a,b_1} \cap F_{a,b_2} = \emptyset$ para todo $a \in A$ y cualesquiera $b_1, b_2 \in B$ con $b_1 \neq b_2$. (Sugerencia: Sea L el conjunto en el lado izquierdo de la igualdad y R el conjunto en el lado derecho. $F_{a,f(a)} \subseteq \bigcup_{b\in B} F_{a,b}$; por lo tanto, $\bigcap_{a\in A} F_{a,f(a)} \subseteq \bigcap_{a\in A}\left(\bigcup_{b\in B} F_{a,b}\right) = L$, y así finalmente $R \subseteq L$. Para probar que $L \subseteq R$, tome $x \in L$. Defina $(a, b) \in f$ si y sólo si $x \in F_{a,b}$. Pruebe que f es una función de A en B para la cual $x \in \bigcap_{a\in A} F_{a,f(a)}$; así, $x \in R$.)

4.3 Productos Cartesianos Arbitrarios

En esta pequeña sección se generaliza el producto cartesiano de conjuntos en términos de funciones. Consideraremos primero casos especiales.

Dados un conjunto no vacío X y un número natural $m \geq 2$, definimos una *m-ada* de elementos de X como una función

$$x : \{1, 2, \ldots, m\} \to X.$$

Si x es una m-ada, es conveniente denotar el valor de x en $i \in \{1, 2, \ldots, m\}$ por x_i en lugar de $x(i)$. Además, representamos la función x por el símbolo

$$(x_1, x_2, \ldots, x_m).$$

En la Sección 3.2 definimos el producto cartesiano de dos conjuntos, introdujimos con base en aquella definición el producto cartesiano de tres conjuntos y únicamente sugerimos la generalización a cuatro conjuntos. En la siguiente definición haremos la primera generalización definiendo el producto cartesiano de una familia de m conjuntos, para cualquier $m \in \mathbf{N}$.

Definición 4.57 Supongamos que $\{A_1, A_2, \ldots, A_m\}$ está indizada sobre el conjunto $\{1, 2, \ldots, , m\}$. El *producto cartesiano de esta familia indizada de conjuntos* denotado por

$$\prod_{i=1}^{m} A_i \qquad \text{o} \qquad A_1 \times A_2 \times \cdots \times A_m$$

es el conjunto de todas las m-adas $(x_1, x_2, x_3, \ldots, x_m)$ de elementos de $X = \bigcup_{i=1}^{m} A_i$ tales que $x_i \in A_i$ para cada $i \in \{1, 2, \ldots, m\}$.

Ejemplo 4.58 Tenemos hasta este momento dos definiciones para el símbolo $A \times B$. Una definición es la dada en la Sección 3.2; según ésta, $A \times B$ denota el conjunto de todos los pares ordenados (a, b) tales que $a \in A$ y $b \in B$. La segunda definición, presentada en esta sección, define a $A \times B$ como el conjunto de todas las funciones $x : \{1, 2\} \to A \cup B$ tales que $x_1 \in A$ y $x_2 \in B$. Hay una obvia correspondencia biyectiva entre estos dos conjuntos: al par (a, b) le hacemos corresponder la función x:$\{1, 2\} \to A \cup B$ definida como $x_1 = a$ y $x_2 = b$. Hemos acordado denotar a esta función con el símbolo (x_1,x_2). Esta notación sugiere en sí misma la correspondencia mencionada.

Podemos generalizar aún más, si $\{A_n\}_{n \in \mathbf{N}}$ es un sistema de conjuntos no vacíos indizado sobre el conjunto de los números naturales $\mathbf{N}$, es factible definir el producto cartesiano de la familia $\{A_n\}$ como:

$$\prod_{n=0}^{\infty} A_n = \left\{ x : \mathbf{N} \to \bigcup_{n=0}^{\infty} A_n : \forall n \in \mathbf{N},\ x_n \in A_n \right\}$$

y como antes representamos las funciones x como:

$$(x_0, x_1, \ldots, x_i, \ldots) \qquad \text{o} \qquad (x_n)_{n=0}^{\infty}.$$

Entonces los elementos de $\prod_{n=0}^{\infty} A_n$ son sucesiones $(x_n)_{n=0}^{\infty}$ de elementos en $\bigcup_{n=0}^{\infty} A_n$ cuyo i-ésimo término, $x_i = x(i)$, pertenece a A_i.

Note que las definiciones anteriores no requieren que los conjuntos A_i sean diferentes uno del otro. De hecho, ellos pueden ser todos iguales a un mismo conjunto A. En este caso, el producto cartesiano $A_1 \times A_2 \times \cdots \times A_m$ es justamente el conjunto A^m de m-adas de elementos en A, y el producto $A_1 \times A_2 \times \cdots$ es justamente el conjunto $A^{\mathbf{N}}$ de todas las sucesiones de elementos en A.

Ejemplo 4.59 $\mathbf{R}^m$ denota el espacio euclidiano m-dimensional. Análogamente, $\mathbf{R}^{\mathbf{N}}$ es algunas veces llamado espacio euclidiano de dimensión infinita. Éste es el conjunto de todas las sucesiones (como se definen en los cursos Cálculo Diferencial e Integral) de números reales; o sea, el conjunto de todas las funciones $x : \mathbf{N} \to \mathbf{R}$.

Ahora pasaremos a la definición más general de producto cartesiano, la cual incluirá estos casos especiales. Primero haremos preciso el significado de *familia indizada de conjuntos*, un concepto que hasta ahora no hemos definido formalmente.

Definición 4.60 Sea $\mathcal{A}$ un sistema de conjuntos. Una *función indizadora* para $\mathcal{A}$ es una función sobreyectiva $A : I \to \mathcal{A}$, donde I es un conjunto no vacío. I es llamado conjunto de índices. La colección $\mathcal{A}$, junto con la función indizadora, es llamada *familia indizada de conjuntos.*

Ejemplo 4.61 Cualquier familia no vacía de conjuntos puede considerarse como una familia indizada de conjuntos, donde la función indizadora es $S : \mathcal{A} \to \mathcal{A}$ dada por $S_A = A$. Ver Observación 3.35.

El principal uso de las funciones indizadoras es para definir el producto cartesiano de familias arbitrarias de conjuntos.

Definición 4.62 Sea $\{A_\alpha\}_{\alpha \in I}$ una familia indizada de conjuntos. El *producto cartesiano de la familia* $\{A_\alpha\}_{\alpha \in I}$, denotado por

$$\prod_{\alpha \in I} A_\alpha,$$

es definido como el conjunto de todas las funciones $x : I \to \bigcup_{\alpha \in I} A_\alpha$, representadas por $(x_\alpha)_{\alpha \in I}$, tales que $x(\alpha) = x_\alpha \in A_\alpha$ para cada $\alpha \in I$. Si $\beta \in I$,

el conjunto A_β es llamado el *β-ésimo factor* del producto $\prod_{\alpha\in I} A_\alpha$. La *coordenada β-ésima* de un elemento $(x_\alpha)_{\alpha\in I}$ en el producto $\prod_{\alpha\in I} A_\alpha$ es por definición $x_\beta = x(\beta)$.

Estamos definiendo un nuevo conjunto; un ejercicio de esta sección es probar que $\prod_{\alpha\in I} A_\alpha$ existe para cualquier familia de conjuntos $\{A_\alpha\}_{\alpha\in I}$ en donde I es un conjunto no vacío. Observemos únicamente que si en la familia $\{B_a\}_{a\in A}$ cada $B_a = B$, el producto $\prod_{a\in A} B_a$ es justamente B^A.

Ejemplo 4.63 Si cada A_α tiene exactamente un elemento, entonces $\prod_{\alpha\in I} A_\alpha$ tiene un elemento.

Ejemplo 4.64 Si $I \neq \emptyset$ y algún $A_\alpha = \emptyset$, entonces $\prod_{\alpha\in I} A_\alpha = \emptyset$.

Ejemplo 4.65 Considere $A_n = \{0, 1\}$ para cada $n \in \mathbf{N}$. El producto cartesiano $\prod_{n\in\mathbf{N}} A_n$ es precisamente el conjunto de todas las sucesiones de ceros y unos, a veces llamado *Conjunto de Cantor.*

Sean $I \neq \emptyset$ y $A_\alpha \neq \emptyset$ para cada $\alpha \in I$. Hasta este momento no podemos asegurar que $\prod_{\alpha\in I} A_\alpha \neq \emptyset$. Aunque intuitivamente esto parece cierto, no es posible demostrarlo sin usar el Axioma de Elección, el cual se abordará en un capítulo posterior. Por el momento *supondremos que* $\prod_{\alpha\in I} A_\alpha \neq \emptyset$ *siempre que* $I \neq \emptyset$ *y* $A_\alpha \neq \emptyset$ *para cada* $\alpha \in I$.

Definición 4.66 Si $\{A_\alpha\}_{\alpha\in I}$ es una familia no vacía de conjuntos no vacíos, se define la *proyección en la β-ésima coordenada* como la función:

$$p_\beta : \prod_{\alpha\in I} A_\alpha \to A_\beta$$

dada por

$$p_\beta\left((x_\alpha)_{\alpha\in I}\right) = x_\beta.$$

Es decir, si $x \in \prod_{\alpha\in I} A_\alpha$, entonces $p_\beta(x) = x(\beta) = x_\beta$.

Con respecto al álgebra de productos cartesianos tenemos el siguiente teorema cuya demostración se deja como un ejercicio.

Teorema 4.67 *Sea $\{X_\alpha\}_{\alpha\in I}$ una familia indizada de conjuntos no vacíos, y sean A_α y B_α subconjuntos no vacíos de X_α, para cada $\alpha \in I$. Entonces:*

(a) $\prod_{\alpha\in I} A_\alpha \cap \prod_{\alpha\in I} B_\alpha = \prod_{\alpha\in I}(A_\alpha \cap B_\alpha)$.

(b) $\prod_{\alpha\in I} A_\alpha \cup \prod_{\alpha\in I} B_\alpha \subseteq \prod_{\alpha\in I}(A_\alpha \cup B_\alpha)$.

Para $\beta \in I$ y $C_\beta \subseteq X_\beta$, denotemos a $p_\beta^{-1}(C_\beta)$ por $\langle C_\beta \rangle$; éste es el "gajo" en $\prod_{\alpha\in I} X_\alpha$ donde cada factor es X_α excepto el β-ésimo, el cual es C_β. Similarmente, para una cantidad finita de índices $\alpha_1, \alpha_2, \ldots, \alpha_m$ y los conjuntos

$$C_{\alpha_1} \subseteq X_{\alpha_1}, \ldots, C_{\alpha_m} \subseteq X_{\alpha_m},$$

el subconjunto $\bigcap_{i=1}^m \langle C_{\alpha_i} \rangle = \bigcap_{i=1}^m p_{\alpha_i}^{-1}(C_{\alpha_i})$ es denotado por

$$\langle C_{\alpha_1}, \ldots, C_{\alpha_i} \rangle .$$

Estas notaciones nos permiten formular el siguiente corolario.

Corolario 4.68 *En* $\prod_{\alpha\in I} X_\alpha$,
(a) $\prod_{\alpha\in I} C_\alpha = \bigcap_{\alpha\in I} \langle C_\alpha \rangle$.
(b) $(\prod_{\alpha\in I} X_\alpha) \setminus \langle C_\beta \rangle = \langle X_\beta \setminus C_\beta \rangle$.
(c) $(\prod_{\alpha\in I} X_\alpha) \setminus (\prod_{\alpha\in I} C_\alpha) = \bigcup_{\alpha\in I} \langle X_\alpha \setminus C_\alpha \rangle$.

DEMOSTRACIÓN:

$c \in \prod_{\alpha\in I} C_\alpha$ si y sólo si para cada $\alpha \in I$, $p_\alpha(c) \in C_\alpha$ si y sólo si para cada $\alpha \in I$, $c \in p_\alpha^{-1}(C_\alpha)$ si y sólo si $c \in \bigcap_{\alpha\in I} \langle C_\alpha \rangle$. Esto establece *(a)*; *(b)* se prueba de manera similar a *(a)*, y *(c)* se sigue de *(a)* y *(b)* usando el Teorema 3.43. ■

Ejercicios 4.3

1. Muestre que existe una correspondencia biyectiva entre $A \times B$ y $B \times A$.

2. Sea $A \times B \times C$ el producto cartesiano de tres conjuntos tal como fue definido en la Sección 3.2, y sea $(A \times B \times C)'$ el producto cartesiano de los tres mismos conjuntos como fue definido en esta sección. Pruebe que existe una biyección $f : A \times B \times C \to (A \times B \times C)'$.

3. Justifique los ejemplos 4.63, 4.64 y 4.65.

4. Pruebe el recíproco del Ejemplo 4.64.

5. (a) Demuestre que existen biyecciones entre $A \times (B \times C)$ y $(A \times B) \times C$.
   (b) Muestre que si $n > 1$, entonces hay una función biyectiva de

$$A_1 \times A_2 \times \cdots \times A_n \quad \text{en} \quad (A_1 \times A_2 \times \cdots \times A_{n-1}) \times A_n.$$

(c) Sea I un conjunto de índices. Pongamos $I = J \cup K$, donde J y K son ajenos y no vacíos. Pruebe que existe una función biyectiva de $\prod_{\alpha\in I} A_\alpha$ en $\prod_{\alpha\in J} A_\alpha \times \prod_{\alpha\in K} A_\alpha$.

6. Sea $I \neq \emptyset$ un conjunto de índices. Considere dos familias indizadas $\{A_\alpha\}_{\alpha\in I}$ y $\{B_\alpha\}_{\alpha\in I}$. Demuestre lo siguiente:

   (a) Si $A_\alpha \subseteq B_\alpha$ para cada $\alpha \in I$, entonces

   $$\prod_{\alpha\in I} A_\alpha \subseteq \prod_{\alpha\in I} B_\alpha.$$

   (b) El recíproco de (a) se cumple si $\prod_{\alpha\in I} A_\alpha \neq \emptyset$.

7. Pruebe que si $\{A_\alpha\}_{\alpha\in I}$ es una familia indizada de conjuntos no vacíos, entonces para cualquier conjunto X y cualquier familia $\{f_\alpha\}$ de funciones $f_\alpha : X \to A_\alpha$, existe una única función

   $$f : X \to \prod_{\alpha\in I} A_\alpha$$

   tal que para cada $\alpha \in I$, $f_\alpha = p_\alpha \circ f$. Las funciones f_α se llaman funciones coordenadas de f, y a veces f se denota por $(f_\alpha)_{\alpha\in I}$ o $\prod f_\alpha$ (ver Ejercicio 4.2.9).

8. Sean m, n enteros positivos y sea $X \neq \emptyset$.

   (a) Para $m \leq n$, encuentre una función inyectiva $f : X^m \to X^n$.
   (b) Encuentre una función biyectiva $g : X^m \times X^n \to X^{m+n}$.
   (c) Encuentre una función inyectiva $h : X^n \to X^{\mathbf{N}}$.
   (d) Encuentre una función biyectiva $k : X^n \times X^{\mathbf{N}} \to X^{\mathbf{N}}$.
   (e) Encuentre una función biyectiva $l : X^{\mathbf{N}} \times X^{\mathbf{N}} \to X^{\mathbf{N}}$.
   (f) Si $A \subseteq B$, encuentre una función inyectiva $m : X^A \to X^B$.

9. Pruebe el Teorema 4.67.

10. Pruebe las partes (b) y (c) del Corolario 4.68.

11. Demuestre que $\prod_{\alpha\in I} A_\alpha \setminus \prod_{\alpha\in I} B_\alpha = \bigcup_{\alpha\in I} Q_\alpha$, donde cada Q_β es un producto cuyo factor $\alpha \neq \beta$ es A_α, y el β-ésimo factor es $A_\beta \setminus B_\beta$.

12. ¿Cuáles de los siguientes subconjuntos de $\mathbf{R}^{\mathbf{N}}$ pueden ser expresados como el producto cartesiano de subconjuntos de $\mathbf{R}$?

    (a) $\{x = (x_n)_{n=0}^{\infty} : x_n \text{ es entero para cada } n \in \mathbf{N}\}$,
    (b) $\{x = (x_n)_{n=0}^{\infty} : x_n \geq n \text{ para cada } n \in \mathbf{N}\}$,
    (c) $\{x = (x_n)_{n=0}^{\infty} : x_n \text{ es un entero para cada } n \geq 100\}$,
    (d) $\{x = (x_n)_{n=0}^{\infty} : x_2 = x_3\}$.

4.4 Equivalencias y Particiones

En esta sección abordaremos dos importantes conceptos. Las nociones de relación de equivalencia y de clases de equivalencia, que fueron primeramente estudiadas en su plena generalidad por Frege [F$_3$] en 1884.

Definición 4.69 Sea R una relación en A.
(a) R es llamada *reflexiva en A,* si para todo $a \in A$, aRa.
(b)[2] R es llamada *simétrica en A,* si para todo $a, b \in A$, aRb implica bRa.
(c) R es llamada *transitiva en A,* si para todo $a, b, c \in A$, aRb *y* bRc implica aRc.

Definición 4.70 Una relación R se llama *de equivalencia en A,* si es reflexiva simétrica y transitiva en A.

Generalmente una relación de equivalencia en A se denota por E, $\equiv$, $\cong$, $\approx$, o $\sim$. Cuando dos elementos $a, b \in A$ satisfacen aEb se dice que a es E-equivalente a b o que a es equivalente a b módulo E. Observe que si E es una relación de equivalencia en A entonces el dominio de E es igual a A; en efecto, la reflexividad implica que para cualquier $a \in A$, $(a, a) \in E$, es decir, $a \in dom\, E$. Por otro lado como E es una relación en A, entonces $E \subseteq A \times A$, por lo que $dom\, E \subseteq A$. Por lo tanto, $dom\, E = A$.

Ejemplo 4.71 Cada una de las relaciones siguientes satisfacen exactamente dos de las propiedades de la Definición 4.69 y, por tanto, no son de equivalencia.
(a) La relación $I^2 = \left\{(x, y) \in \mathbf{R}^2 : 0 \leq x \leq 1,\ 0 \leq y \leq 1\right\}$ en $\mathbf{R}$, no es reflexiva.
(b) La relación $R_1 = \left\{(x, y) \in \mathbf{R}^2 : x \leq y\right\}$ en $\mathbf{R}$, no es simétrica.
(c) La relación $R_2 = \left\{(x, y) \in \mathbf{R}^2 : |x - y| \leq 1\right\}$ en $\mathbf{R}$ no es transitiva.

[2] $a, b \in A$ significa $a \in A$ y $b \in A$.

Ejemplo 4.72 La relación vacía en un conjunto A es simétrica y transitiva, pero no reflexiva salvo que $A = \emptyset$.

Ejemplo 4.73 Sea P el conjunto de todas las personas que viven en la tierra. Decimos que una persona p es equivalente a q *($p \cong q$)* si ambos p y q viven en el mismo país. Trivialmente $\cong$ es reflexiva, simétrica y transitiva en P.

Note que el conjunto P del ejemplo anterior puede ser "partido" en clases de elementos mutuamente equivalentes; toda la gente que vive en México forman una de estas clases, todas las personas que viven en Francia forman otra clase, etc. Todos los miembros de una misma clase son equivalentes. Las clases de equivalencia corresponden exactamente a los diferentes países.

Ejemplo 4.74 Defina la relación $\equiv$ en el conjunto de los enteros $\mathbf{Z}$ como sigue*:* $x \equiv y$ si y sólo si $y - x$ es divisible[3] por 2. Se puede verificar fácilmente que $\equiv$ cumple (a), (b) y (c) de la Definición 4.69, es decir, $\equiv$ es una equivalencia.

Nuevamente el conjunto $\mathbf{Z}$, puede ser dividido en clases de equivalencia bajo $\equiv$. En este caso, hay dos clases de equivalencia: el conjunto de los enteros pares y el conjunto de los enteros impares. Cualesquiera dos pares o cualesquiera dos impares están relacionados, pero nunca un par está relacionado con un impar.

Los ejemplos anteriores reflejan una regla general; una relación de equivalencia en un conjunto A genera una partición del conjunto A en clases de equivalencia; recíprocamente, dada una partición en A hay una equivalencia en A determinada por la partición de A.

Definición 4.75 Sea E una equivalencia en A y sea $a \in A$. La *clase de equivalencia de a módulo E* es el conjunto

$$[a] = \{x \in A : xEa\}.$$

Obsérvese que efectivamente lo que hemos llamado clase de equivalencia de a, es un conjunto. Por el peso de la tradición histórica llamamos clase a $[a]$, aquí el término *clase* es diferente al usado en la Convención 2.5. Es conveniente también notar que para todo $a \in A$, $[a] \neq \emptyset$, pues al menos $a \in [a]$.

Cuando se trabaja con varias relaciones en un mismo conjunto A, es preferible emplear la notación Ea para denotar la clase de equivalencia de a módulo E.

---

[3] m es divisible por n si existe $k \in \mathbf{Z}$ tal que $m = k \cdot n$.

Ejemplo 4.76 En $\mathbf{Z}$ se define la congruencia módulo n como $a \equiv b \bmod n$ si y sólo si $b - a$ es divisible por n. $\equiv$ es una relación de equivalencia y la clase de equivalencia de $a \in \mathbf{Z}$ es el conjunto $\{a + kn : k \in \mathbf{Z}\}$.

Lema 4.77 *Sean E una equivalencia en A y $a, b \in A$.*
(a) a es equivalente a b módulo E si y sólo si $[a] = [b]$.
(b) a no es equivalente a b módulo E si y sólo si $[a] \cap [b] = \emptyset$.

Demostración:

(a) Supóngase que aEb. Sea $x \in [a]$, entonces xEa y aEb. Por la transitividad de E, xEb, lo que significa $x \in [b]$. Similarmente $x \in [b]$ implica $x \in [a]$. Así, $[a] = [b]$.

(b) Supongamos que no ocurre aEb, y que existe $x \in [a] \cap [b]$. Entonces xEa y xEb, y en virtud de la reflexividad y transitividad de E, aEb. Esto contradice el supuesto.

Por último supongamos que $[a] \cap [b] = \emptyset$. Si ocurriera aEb, entonces $a \in [b]$. Pero $a \in [a]$, lo que contradice la relación $[a] \cap [b] = \emptyset$. ■

Definición 4.78 Una familia de conjuntos $\mathcal{F}$ no vacíos se llama *partición de A* si:

(a) Los conjuntos que forman $\mathcal{F}$ son ajenos dos a dos, es decir, $C, D \in \mathcal{F}$ y $C \neq D$ implica $C \cap D = \emptyset$.

(b) La unión de $\mathcal{F}$ es A, es decir, $A = \bigcup \mathcal{F}$.

Definición 4.79 Sea E una relación de equivalencia en A. La familia de todas las clases de equivalencia módulo E es denotada por A/E y

$$A/E = \{[a] : a \in A\}.$$

Usualmente a A/E se le llama *conjunto cociente de A por la relación E*.

Teorema 4.80 *Sea E una equivalencia, entonces A/E es una partición de A.*

Demostración:

La parte (a) de la Definición 4.78 se sigue del Lema 4.77: si $[a] \neq [b]$, entonces a y b no son equivalentes módulo E, así $[a] \cap [b] = \emptyset$. Para probar (b), note que $A = \bigcup A/E$ porque $a \in [a]$ para cada $a \in A$. Además, por la misma razón, no hay clases de equivalencia vacías. ■

Definición 4.81 Sea $\mathcal{F}$ una partición de A. La relación $E_{\mathcal{F}}$ determinada por $\mathcal{F}$ es definida por:

$$E_{\mathcal{F}} = \{(a,b) \in A \times A : \exists B \in \mathcal{F} \text{ tal que } a,b \in B\}.$$

La definición de la relación $E_{\mathcal{F}}$ puede hacerse en otras palabras: $a, b \in A$ están $E_{\mathcal{F}}$-relacionados si y sólo si ellos pertenecen al mismo elemento de la partición $\mathcal{F}$.

Teorema 4.82 *Sea $\mathcal{F}$ una partición de A. Entonces $E_{\mathcal{F}}$ es una relación de equivalencia en A.*

Demostración:

(a) Reflexividad. Sea $a \in A$. Puesto que $A = \bigcup \mathcal{F}$, entonces existe $C \in \mathcal{F}$ tal que $a \in C$, así; $(a,a) \in E_{\mathcal{F}}$.

(b) Simetría. Supóngase que $(a,b) \in E_{\mathcal{F}}$, entonces existe $C \in \mathcal{F}$ tal que $a \in C$ y $b \in C$. Por lo cual $b \in C$ y $a \in C$; lo cual implica $(b,a) \in E_{\mathcal{F}}$.

(c) Transitividad. Supongamos que $(a,b) \in E_{\mathcal{F}}$ y $(b,c) \in E_{\mathcal{F}}$, entonces existen conjuntos $C, D \in \mathcal{F}$ tales que $a, b \in C$ y $b, c \in D$. Como los elementos de $\mathcal{F}$ son mutuamente ajenos entonces $D = C$, por lo que $a, c \in D$ y así $(a,c) \in E_{\mathcal{F}}$. ■

El siguiente teorema, que establece la relación entre equivalencias y particiones, se demuestra de modo análogo.

Teorema 4.83 *(a) Si E es una relación de equivalencia en A y $\mathcal{F} = A/E$, entonces $E = E_{\mathcal{F}}$.*

(b) Si $\mathcal{F}$ es una partición de A y $E_{\mathcal{F}}$ es la correspondiente relación de equivalencia determinada por $\mathcal{F}$, entonces $\mathcal{F} = A/E_{\mathcal{F}}$.

Así las relaciones de equivalencia y las particiones son dos descripciones diferentes del mismo concepto. Toda equivalencia E determina una partición $\mathcal{F} = A/E$. La equivalencia $E_{\mathcal{F}}$ determinada por la partición $\mathcal{F} = A/E$ es idéntica a la original. Recíprocamente, cada partición determina una relación de equivalencia; cuando formamos las clases de equivalencia módulo $E_{\mathcal{F}}$, recobramos la partición original.

Cuando trabajamos con equivalencias o particiones, es muy conveniente tener un conjunto que consista precisamente de un elemento de cada clase de equivalencia.

Definición 4.84 Sea E una relación de equivalencia en A. Un conjunto $X \subseteq A$ es llamado *conjunto de representantes para las clases de equivalencia módulo*

E (o para una partición $\mathcal{F}$), si para todo $C \in A/E$ *($C \in \mathcal{F}$),* $X \cap C = \{a\}$ para algún $a \in C$.

Ejemplo 4.85 Para la relación de equivalencia definida en el Ejemplo 4.73, el conjunto X de los presidentes o jefes de estado de cada país son un conjunto de representantes. El conjunto $X = \{0, 1\}$ lo es para la relación de equivalencia del Ejemplo 4.74.

¿Cualquier partición tiene un conjunto de representantes? Intuitivamente la respuesta es sí, pero, nuevamente, sin el Axioma de Elección, es imposible probar tal afirmación. Es decir, necesitamos usar el Axioma de Elección para demostrar la existencia de un conjunto de representantes, salvo para relaciones simples. En el siguiente ejemplo se muestra una relación de equivalencia para la cual la existencia de un conjunto de representantes no es obvia.

Ejemplo 4.86 Sea $I = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$. La relación $\equiv$ definida por $a \equiv b$ si y sólo si la diferencia $a - b$ es un número racional, es una relación de equivalencia.[4]

Definición 4.87 Sean A un conjunto y E una relación de equivalencia en A. La función que asigna a cada elemento de A su clase de equivalencia módulo E, es decir, $p_E : A \to A/E$ tal que $p_E(a) = Ea$, se llama *función proyección* o *proyección natural.*

El que $p_E : A \to A/E$ sea una función puede deducirse del Lema 4.77; en efecto, para $a \in A$, $(a, Eb) \in p_E$ y $(a, Ec) \in p_E$ implica $a \in Eb$ y $a \in Ec$ con lo cual $Eb \cap Ec \neq \emptyset$; así $Eb = Ec$. Claramente p_E es una función sobreyectiva, pero en general no es inyectiva (puesto que $Ea = Eb$ siempre que aEb).

Definición 4.88 Sean A, B dos conjuntos y sean R, S relaciones de equivalencia en A y en B, respectivamente. Una función $f : A \to B$ *preserva las relaciones R y S*, si aRb implica $f(a)Sf(b)$.

Teorema 4.89 *Sea $f : A \to B$ una función que preserva las relaciones R y S. Entonces existe una única función $f_* : A/R \to B/S$ tal que $p_S \circ f = f_* \circ p_R$. A f_* se le llama función inducida por f en "el paso al cociente".*

---

[4]Este ejemplo se debe a Vitali [V] quien probó que ninguno de los conjuntos de representantes de la relación definida en el ejemplo es medible según Lebesgue (ver Ejemplo 8.18).

DEMOSTRACIÓN:

Definamos $f_* : A/R \to B/S$ como $f_*(Ra) = Sf(a)$ para cada $Ra \in A/R$. Veamos primero que f_* está bien definida. La función f_* asigna a Ra el único (por el Lema 4.77) elemento $Sb \in B/S$ tal que $f(a) \in Sb$. Así entonces, para ver que f_* está bien definida es suficiente con mostrar que la clase $Sf(a)$ no depende del representante a seleccionado. Si $Ra = Ra'$, por el Lema 4.77, aRa'. Puesto que f preserva relaciones, tenemos que $f(a)Sf(a')$. Por lo tanto, f_* está unívocamente definida. El dominio de f_* es A/R ya que A es el dominio de f y p_R es sobreyectiva.

Por otro lado,

$$(p_S \circ f)(a) = p_S(f(a)) = Sf(a) = f_*(Ra) = f_*(p_R(a)) = (f_* \circ p_R)(a),$$

lo cual significa que $p_S \circ f = f_* \circ p_R$ (véase el Lema 4.35). Finalmente, f_* es única puesto que p_R es sobreyectiva: si g_* fuera otra función tal que $p_S \circ f = g_* \circ p_R$, entonces $f_* \circ p_R = g_* \circ p_R$ y, por el Teorema 4.49(e), $f_* = g_*$. Por lo tanto, que f_* es única. ■

El recíproco del teorema anterior también es válido, esto es: si $f : A \to B$ y $f' : A/R \to B/S$ son funciones tales que $p_S \circ f = f' \circ p_R$, entonces f necesariamente preserva las relaciones, y $f' = f_*$. En efecto, supongamos que f y f' son dos funciones tales que $p_S \circ f = f' \circ p_R$. Sean $a, a' \in A$ con aRa', entonces $p_R(a) = p_R(a')$ y puesto que $p_S \circ f = f' \circ p_R$, tenemos que $(p_S \circ f)(a) = (p_S \circ f)(a')$. Esto muestra que $f(a)Sf(a')$ y prueba que f preserva las relaciones. Que $f' = f_*$ se sigue de la unicidad de f_* en el teorema anterior.

Ejemplo 4.90 Sean $A = B = \mathbf{Z}$. Sea R la congruencia módulo 4 y sea S la congruencia módulo 2 del Ejemplo 4.76. Entonces $f : A \to B$ dada por $f(n) = n$, preserva las relaciones. Usando el conjunto de representantes $\{0, 1, 2, 3\}$ para A/R y $\{0, 1\}$ para B/S, es fácil verificar que $f_*(0) = f_*(2) = 0$ y $f_*(1) = f_*(3) = 1$.

Muchas de las aplicaciones de las relaciones de equivalencia en matemáticas están en la dirección de formular nociones matemáticas, o como usualmente se dice, formalizar las definiciones por abstracción. La esencia de esta técnica es definir una noción como el conjunto de todos los objetos los cuales se desea tengan la cualidad para la noción. Por ejemplo, en un capítulo posterior definiremos un concepto extremadamente necesario en las matemáticas, como es el de número real. La técnica en este caso particular será definiendo relaciones de equivalencia, primero en el conjunto de los números naturales, después en el conjunto cociente, y más aún, en el "cociente del cociente" para

llegar a definir los números racionales y finalmente definir otra relación de equivalencia para llegar a definir "un número real".

Ejercicios 4.4

1. Sea X un conjunto. Pruebe que la relación $\subseteq$ en $\mathcal{P}(X)$ es siempre reflexiva y transitiva. Pruebe también que es simétrica si y sólo si $X = \emptyset$.

2. Aquí damos una "demostración" de que toda relación R en un conjunto A que es a la vez simétrica y transitiva, es también reflexiva: "Como R es simétrica, aRb implica bRa. Ahora, dado que R es transitiva, aRb y bRa juntas implican aRa, como se deseaba." Encuentre el error de este argumento.

3. Pruebe que una relación E en A es de equivalencia si y sólo si $Id_A \subseteq E$, $E = E^{-1}$ y $E = E \circ E$.

4. Si R es una relación reflexiva y transitiva en $A = dom\, R$, muestre que $E = R \cap R^{-1}$ es una relación de equivalencia en A.

5. Verifique las afirmaciones del Ejemplo 4.71.

6. Verifique las afirmaciones del Ejemplo 4.76.

7. Considere la relación E en $\mathbf{R}^2$ definida por

$$E = \left\{((x_1, y_1), (x_2, y_2)) : y_1 - (x_1)^2 = y_2 - (x_2)^2\right\}.$$

   Muestre que E es una relación de equivalencia y describa las clases de equivalencia módulo E.

8. Sean E y E' las siguientes relaciones en $\mathbf{R}$:

$$E = \{(x, y) : y = x + 1\} \qquad , \qquad E' = \{(x, y) : y - x \in \mathbf{Z}\}.$$

   (a) Muestre que E' es una relación de equivalencia en $\mathbf{R}$ y que $E \subseteq E'$.

   (b) Describa las clases de equivalencia módulo E'.

   (c) ¿Es E una relación de equivalencia?

9. Sea $f : X \to Y$ una función. Muestre que:

(a) $E_f = \{(x, y) : f(x) = f(y)\}$ es una relación de equivalencia en X.
(b) Las clases de equivalencia módulo E_f son precisamente los conjuntos $f^{-1}(\{y\})$ para $y \in f(X)$.

10. Sean $f : A \to B$ una función y E una relación de equivalencia en B. Pruebe que
$$f^{\leftarrow}(E) = \left\{(x, y) \in A^2 : f(x)Ef(y)\right\}$$
es una relación de equivalencia en A.

11. Para relaciones R, S en A y B, respectivamente, defina $R \times S$ en $A \times B$ por
$$R \times S = \{((a, b), (c, d)) : aRc \ \wedge \ bSd\}.$$
Si R, S son relaciones de equivalencia, pruebe que $R \times S$ es una relación de equivalencia en $A \times B$.

12. Sean S y R relaciones de equivalencia en A, con $S \subseteq R$. Defina
$$R/S = \left\{(Sa, Sb) : \exists a' \in Sa, \ \exists b' \in Sb \text{ tales que } (a', b') \in R\right\}.$$
Muestre que R/S es una relación de equivalencia en el conjunto cociente A/S y que hay una biyección de $(A/S)/(R/S)$ en A/R. (Sugerencia: demuestre primero que $S_a \subseteq R_a$ para cada $a \in A$. Para construir la biyección use 4.89.)

13. Demuestre que una relación R en A es de equivalencia si y sólo si existe una partición $\{A_\alpha\}_{\alpha \in I}$ de A tal que
$$R = \bigcup \{A_\alpha \times A_\alpha : \alpha \in I\}.$$
Más aún, los conjuntos A_α son precisamente las clases de equivalencia módulo R.

14. Pruebe que si A es un conjunto y E es una relación de equivalencia en A, entonces A/E es un conjunto.

15. Sean $\mathcal{A}$ y $\mathcal{B}$ dos particiones de X. Demuestre que la condición $E_{\mathcal{A}} \subseteq E_{\mathcal{B}}$ es equivalente a: cualquier conjunto $A \in \mathcal{A}$ es la unión de una familia $\mathcal{A}' \subseteq \mathcal{B}$.

16. Sea $I = \{x \in \mathbf{R} : 0 \leq x \leq 1\}$. Para $X \subseteq I$ denótese por $X(r)$ el conjunto de números pertenecientes a I que tienen la forma $x + r + n$, donde $x \in X$ y n es un número entero. Demuestre que, si Z es un conjunto de representantes para la relación $\equiv$ definida por $a \equiv b$ si y sólo si $a - b \in \mathbf{Q}$ entonces:

(a) $Z(r) \cap Z(s) = \emptyset$ para cualesquiera números racionales r, s con $r \neq s$.

(b) $I = \bigcup_{r \in \mathbf{Q}} Z(r)$.

17. Muestre que si $\mathcal{M}$ es una familia no vacía de relaciones de equivalencia en A, entonces $\bigcap \mathcal{M}$ es una relación de equivalencia en A.

18. Preservando la notación del Ejercicio 17 pruebe que existe una relación de equivalencia E en A tal que

    (a) $R \in \mathcal{M}$ implica $R \subseteq E$,

    (b) si E' es una relación de equivalencia en A y $\forall R \in \mathcal{M}$, $R \subseteq E'$, entonces $E \subseteq E'$.

19. Si $\mathcal{M} = \{E_{\mathcal{A}}, E_{\mathcal{B}}\}$, describa $\bigcup \mathcal{M}$ y la relación E cuya existencia se asegura en el ejercicio anterior.

4.5 Órdenes

Otro de los conceptos fundamentales en matemáticas es el concepto de orden en un conjunto. Un orden puede ser definido como una relación con características especiales.

Definición 4.91 Una relación R en A es antisimétrica si para todo $a, b \in A$, aRb y bRa implica $a = b$.

Definición 4.92 Una relación R en A, que es reflexiva, antisimétrica y transitiva se llama orden (parcial) en A. El par (A, R) se le llama conjunto (parcialmente) ordenado.

Primero note que el dominio de un orden en A es A. A aRb se le puede leer como: "a es menor o igual que b", "b es mayor o igual que a", " a precede a b" o "b es sucesor de a" (en el orden R). Así, todo elemento de A es menor (mayor) o igual a sí mismo. Generalmente se usan los símbolos $\leq$, $\preceq$, $\ll$, para denotar órdenes.

Ejemplo 4.93 La relación vacía $\emptyset$, en cualquier conjunto A no es un orden, salvo que $A = \emptyset$.

Ejemplo 4.94 Dado un conjunto A, la relación identidad es un orden.

Ejemplo 4.95 Si $\leq$ es el orden usual en el conjunto de los números reales, entonces $\leq$ es un orden según la Definición 4.92.

Ejemplo 4.96 La relación definida por $m \mid n$ si y sólo si m divide a n, es un orden en el conjunto de los números enteros positivos.

Ejemplo 4.97 Si X es un conjunto, la contención de conjuntos es un orden en $\mathcal{P}(X)$.

Ejemplo 4.98 La relación de pertenencia $\in_A$ restringida a un conjunto A no es un orden, pues no es reflexiva (ver Definición 4.25 y Teorema 2.33).

Ejemplo 4.99 Sea $\mathbf{C}$ el conjunto de los números complejos ($z = a + ib$ con $a, b \in \mathbf{R}$), y definamos $z_1 \preceq z_2$ si y sólo si $\|z_1\| \leq \|z_2\|$, donde $\leq$ es el orden usual de los números reales y $\|z\| = \sqrt{a^2 + b^2}$. Entonces la relación $\preceq$ es reflexiva y transitiva, pero no antisimétrica. Por lo tanto, no es un orden parcial en $\mathbf{C}$. A las relaciones como $\preceq$ que son reflexivas y transitivas se les llama *pre-órdenes*.

Algunas veces es conveniente modificar una relación de orden como sigue: en lugar de la relación $\leq$ entre números, se puede preferir el uso de la relación $<$ (estrictamente menor). Similarmente, se usará $\subset$ (subconjunto propio) en lugar de $\subseteq$, es decir, $A \subseteq B$ y $A \neq B$.

Definición 4.100 Una relación S en A es *asimétrica* si para todo $a, b \in A$, aSb implica que no ocurre bSa. Es decir, (a, b) y (b, a) no pueden ser ambos elementos de S.

Definición 4.101 Una relación S en A es un orden estricto, si es asimétrica y transitiva.

Ejemplo 4.102 Para cualquier conjunto A, la relación $\emptyset$ es un orden estricto en A.

Teorema 4.103 *(a) Sea R un orden en A, entonces la relación S definida en A por aSb si y sólo si aRb y $a \neq b$, es un orden estricto en A.*

(b) Sea S un orden estricto en A, entonces la relación R definida en A por aRb si y sólo si aSb o $a = b$ es un orden en A.

Así podemos decir que los órdenes estrictos S corresponden a órdenes R y viceversa.

Ejemplo 4.104 Sean $A \neq \emptyset$ y $S = \emptyset$. Entonces el orden R obtenido en el teorema anterior es la relación identidad, Id_A.

Obsérvese que si R es un orden en A no necesariamente para cualesquiera $a, b \in A$, ocurre que aRb o bRa, aún cumpliéndose que $dom\, R = A$.

Definición 4.105 Sean $a, b \in A$ y sea $\leq$ un orden en A. Decimos que a y b son *comparables en el orden* $\leq$ (o que son $\leq$-*comparables*) si:

$$a \leq b \quad o \quad b \leq a.$$

Decimos que a y b son $\leq$-*incomparables* si no son $\leq$-comparables. Similarmente se define para un orden estricto $<$ las nociones de $<$-comparables y $<$-incomparables; por ejemplo, a y b son $<$-comparables si; $a < b$, $a = b$ o $b < a$.

Ejemplo 4.106 Cualesquiera dos números reales son comparables en el orden usual $\leq$.

Ejemplo 4.107 2 y 3 son incomparables en el orden $|$ del Ejemplo 4.96.

Ejemplo 4.108 Cualesquiera $a, b \in X$ con $a \neq b$ son incomparables en el orden Id_X.

Ejemplo 4.109 Si A tiene al menos dos elementos, entonces hay elementos incomparables en el conjunto ordenado $(\mathcal{P}(A), \subseteq)$.

Definición 4.110 Un orden $\leq$ (o $<$) es llamado *lineal* o *total* si cualesquiera dos elementos de A son comparables. El par $(A, \leq)$ es entonces llamado *conjunto linealmente* o *totalmente ordenado*.[5]

Ejemplo 4.111 El orden usual $\leq$ en los números enteros es lineal, mientras que $|$ no lo es.

Ejemplo 4.112 Sean $(A, \leq)$ y $(B, \preceq)$ dos conjuntos linealmente ordenados, entonces definiendo en $A \times B$ las siguientes relaciones tenemos ordenes lineales para $A \times B$. La primera llamada orden lexicográfico vertical es: $(a_1, b_1) \ll_v (a_2, b_2)$ si y sólo si $(a_1 < a_2)$ o $(a_1 = a_2$ y $b_1 \preceq b_2)$. La segunda, el orden lexicográfico horizontal: $(a_1, b_1) \ll_h (a_2, b_2)$ si y sólo si $(b_1 < b_2)$ o $(b_1 = b_2$ y $a_1 \leq a_2)$.

Ejemplo 4.113 El conjunto $\mathbf{C}$ de los números complejos con cualquiera de los órdenes lexicográficos es totalmente ordenado.[6]

---

[5]Lor órdenes lineales fueron considerados originalmente por Cantor [C_1]. Los órdenes parciales fueron introducidos por Hausdorff [H_4].

[6]Esto no quiere decir que los números complejos sean un campo ordenado; de hecho, eso es imposible. Para la definición de campo ordenado vea la página 206.

Definición 4.114 Sea $B \subseteq A$, donde A está ordenado por $\leq$. B es una *cadena en* $(A, \leq)$ si cualesquiera dos elementos de B son $\leq$-comparables.

Por ejemplo el conjunto de todas las potencias de 2, $\left\{2^0, 2^1, 2^2, \ldots\right\}$, es una cadena en el conjunto de los enteros positivos ordenado por divisibilidad.

Es evidente que un orden parcial (respectivamente total) induce un orden parcial (respectivamente total) en cualquier subconjunto; así, una cadena en un conjunto ordenado $(A, \leq)$ es un subconjunto totalmente ordenado en el orden inducido.

Definición 4.115 Sea $\leq$ un orden en A, y sea $B \subseteq A$.

(a) $b \in B$ es el *elemento mínimo de* B en el orden $\leq$, si para todo $x \in B$, $b \leq x$.

(b) $b \in B$ es un *elemento minimal de* B en el orden $\leq$, si no existe $x \in B$ tal que $x \leq b$ y $x \neq b$.

(c) $b \in B$ es el *elemento máximo de* B en el orden $\leq$, si para todo $x \in B$, $x \leq b$.

(d) $b \in B$ es un *elemento maximal de* B en el orden $\leq$, si no existe $x \in B$ tal que $b \leq x$ y $x \neq b$.

Obsérvese el empleo del artículo *el* en las partes *(a)* y *(c)*, y el empleo del artículo *un* en las partes *(b)* y *(d)*. Esta diferencia en el empleo de los diferentes artículos es necesaria. Primeramente, en virtud de la antisimetría, los elementos mínimo y máximo (si existen) son únicos; no sucede así con los minimales y maximales. La razón es que la definición de mínimo y máximo implica que estos elementos son comparables con todo elemento de B, mientras que las definiciones de minimal y maximal no implican que estos elementos (si existen) necesariamente deban ser comparables con cualquier elemento de B. De hecho, cuando un conjunto B tiene dos elementos maximales, estos son incomparables.[7] Veamos algunos ejemplos.

Ejemplo 4.116 Sea $\mathbf{Z}^+$ el conjunto de todos los enteros positivos ordenado por $\mid$. Entonces 1 es el elemento mínimo de $\mathbf{Z}^+$, pero $\mathbf{Z}^+$ no tiene elemento máximo. Si $B = \mathbf{Z}^+ \setminus \{1\}$, entonces B no tiene elemento mínimo en el orden $\mid$ (2 no es el mínimo porque $2 \mid 3$ falla); pero este conjunto tiene muchos (infinitos) elementos minimales, a saber, 2, 3, 5, 7, etc. (exactamente todos los números primos) son minimales. B no tiene ni máximo ni maximales.

[7] En castellano no se emplean las palabras maximal y minimal. Algunas traducciones prefieren utilizar los términos "elemento máximo" y "elemento mínimo" como nombres para tales conceptos; "máximo" y "mínimo" para el elemento máximo y mínimo. Creemos que la terminología aquí empleada evita confusiones.

Ejemplo 4.117 Sea A cualquier conjunto con el orden dado por la relación identidad, Id_A. Si $B \subseteq A$ entonces cualquier elemento de B es tanto minimal como maximal.

En el siguiente teorema se encuentran algunas propiedades de los elementos mínimo y minimal. La demostración se deja como un ejercicio.

Teorema 4.118 *Sean A ordenado por $\leq$, y $B \subseteq A$.*

(a) B tiene a lo más un elemento mínimo.

(b) El elemento mínimo de B (si existe) es también minimal.

(c) Si B es una cadena, entonces todo elemento minimal de B es también un mínimo.

El teorema es también válido si las palabras "mínimo" y "minimal" son reemplazadas por "máximo" y "maximal", respectivamente.

Definición 4.119 Sean $\leq$ un orden en A y $B \subseteq A$.

(a) $a \in A$ es una *cota inferior de* B en el conjunto ordenado $(A, \leq)$, si $a \leq x$ para todo $x \in B$.

(b) $a \in A$ es llamado *ínfimo de* B en $(A, \leq)$ (o *máxima cota inferior*), si es el elemento máximo del conjunto de todas las cotas inferiores de B en $(A \leq)$.

(c) $a \in A$ es una *cota superior* de B en el conjunto ordenado $(A, \leq)$, si $x \leq a$ para todo $x \in B$.

(d) $a \in A$ se llama *supremo de* B en $(A, \leq)$ (o *mínima cota superior*), si es el elemento mínimo del conjunto de todas las cotas superiores de B en $(A, \leq)$.

La diferencia entre "a es el mínimo de B" y "a es una cota inferior de B", es que el segundo concepto no requiere que $a \in B$. Un conjunto puede tener muchas cotas inferiores; pero el conjunto de todas las cotas inferiores de B puede tener a lo más un elemento máximo. Así, B puede tener a lo más un ínfimo. Similar observación puede hacerse para máximo, cota superior y supremo. A continuación expresamos formalmente estas ideas.

Teorema 4.120 *Sean $(A, \leq)$ un conjunto ordenado y $B \subseteq A$.*

(a) B tiene a lo más un ínfimo.

(b) Si b es el elemento mínimo de B, entonces b es ínfimo de B.

(c) Si b es el ínfimo de B y $b \in B$, entonces b es el elemento mínimo de B.

(d) $b \in A$ es el ínfimo de B en $(A, \leq)$ si y sólo si

(i) $b \leq x$, para todo $x \in B$, y

(ii) si $b' \leq x$, para todo $x \in B$, entonces $b' \leq b$.

El teorema es válido si las palabras "mínimo" e "ínfimo" son reemplazadas por "máximo" y "supremo" y "$\leq$" es reemplazado por "$\geq$" en (i) y (ii).

DEMOSTRACIÓN:

(a) Está prácticamente probada en la observación que precede al teorema.

(b) El mínimo elemento de B es ciertamente una cota inferior de B. Si b' es cualquier otra cota inferior de B, $b' \leq b$ puesto que $b \in B$. Así, b es el elemento máximo del conjunto de todas las cotas inferiores de B.

(c) Es obvio.

(d) Esta es sólo una reformulación de la definición de ínfimo. ■

Empleando los Teoremas 4.118 y 4.120 podemos usar una notación para denotar mínimo, máximo, ínfimo y supremo de un subconjunto B en un conjunto ordenado $(A, \leq)$. La notación comúnmente empleada es: $\min B$, $\max B$, $\inf B$ y $\sup B$, respectivamente.

Ejemplo 4.121 Sea $\leq$ el orden usual en el conjunto de los números reales. Analicemos los conjuntos $B_1 = \{x \in \mathbf{R} : 0 < x < 1\}$, $B_2 = \{x \in \mathbf{R} : 0 \leq x < 1\}$, $B_3 = \{x \in \mathbf{R} : x > 0\}$, $B_4 = \{x \in \mathbf{R} : x < 0\}$. B_1 no tiene elemento máximo ni elemento mínimo, pero cualquier $b \leq 0$ es una cota inferior; así, 0 es la máxima cota inferior de B_1, es decir, $\inf B_1 = 0$. Similarmente, cualquier $b \geq 1$ es cota superior de B_1, y $\sup B_1 = 1$. El conjunto B_2 tiene elemento mínimo, $\min B_2 = 0$, pero no tiene máximo; sin embargo, $\sup B_2 = 1$. El conjunto B_3 no tiene elemento máximo y tampoco tiene supremo; de hecho, B_3 no es acotado superiormente en $(\mathbf{R}, \leq)$; $\inf B_3 = 0$. Similarmente, B_4 no tiene cotas inferiores y, por tanto, no tiene ínfimo.

Ejemplo 4.122 Un conjunto puede ser acotado superiormente y no tener supremo. Considérese $X = \mathbf{R} \setminus \{0\}$ y sea

$$B = \{x \in X : x \text{ es negativo}\}.$$

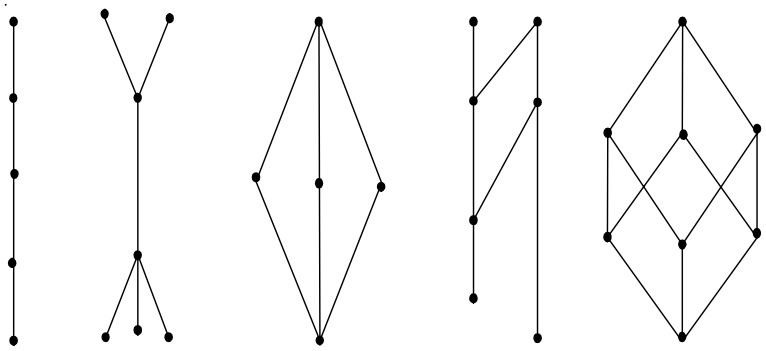
Entonces B es acotado superiormente, pero no tiene supremo en el conjunto ordenado $(X, \leq)$, donde $\leq$ es el orden usual en los números reales.

Si tenemos un conjunto ordenado finito $(A, \leq)$, entonces $x < y$ si y sólo si existe una cadena de la forma

$$x = x_1 < x_2 < \cdots < x_n = y.$$

El resultado anterior permite representar a cualquier conjunto ordenado finito por medio de un diagrama. Los elementos de A son representados por puntos acomodados acorde con la siguiente regla: el punto x_2 es colocado arriba del punto x_1 si y sólo si $x_1 < x_2$, y si no existen otros elementos de A que sean

sucesor de x_1 y precedan a x_2, los puntos son unidos por un segmento de línea. Así, $x < y$ si y sólo si existe una línea quebrada ascendente que conecta a x y y. Algunos ejemplos de tales diagramas son mostrados en la figura (4.5.1).



(4.5.1)

El primero es el diagrama de una cadena de cinco elementos. Claramente, el diagrama de cualquier cadena tiene esta forma. El último de los diagramas corresponde al conjunto potencia de un conjunto con tres elementos, ordenado por la inclusión; el punto en el nivel más bajo representa al conjunto vacío, los puntos del siguiente nivel representan los subconjuntos unitarios, y así sucesivamente. Tales diagramas no sólo sirven para representar un conjunto ordenado por una figura que muestre la relación de orden, también pueden ser usados para definir conjuntos ordenados: la relación de orden es justamente la indicada por la variedad de líneas quebradas.

Para preparar nuestra siguiente definición que relaciona conjuntos ordenados, discutiremos un ejemplo. Considere el conjunto

$$\{1, 2, 3, 5, 6, 10, 15, 30\},$$

cuyos miembros son los divisores positivos de 30, ordenados por la relación $\leq$, donde $x \leq y$ si y sólo si x es múltiplo de y. Se deja como un ejercicio mostrar que el diagrama de este conjunto ordenado es idéntico al diagrama asociado a los subconjuntos de un conjunto de tres elementos ordenado por la contención. A pesar de que estos conjuntos ordenados son distintos, ellos son indistinguibles en su estructura como conjuntos ordenados. Es ciertamente notable que exista este tipo de relaciones entre dos conjuntos ordenados ya que cualquier propiedad de uno que sea expresable en términos de su relación de orden tiene una análoga en el otro conjunto. La identidad de los diagramas de los dos conjuntos ordenados antes mencionados implican, primero: la existencia de una biyección entre los conjuntos; segundo: que la relación de orden entre dos elementos de uno de los conjuntos, es la misma que para el correspondiente par de elementos en el otro conjunto.

Definición 4.123 Un *isomorfismo* entre dos conjuntos ordenados $(P, \leq)$ y $(Q, \preceq)$ es una función biyectiva $h : P \to Q$ tal que para todo $p_1, p_2 \in P$,

$$p_1 \leq p_2 \text{si y sólo si } h(p_1) \preceq h(p_2).$$

Si existe un isomorfismo entre $(P, \leq)$ y $(Q, \preceq)$, entonces $(P, \leq)$ y $(Q, \preceq)$ son *isomorfos* y la biyección h se llama *isomorfismo* entre $(P, \leq)$ y $(Q, \preceq)$.

La expresión "si y sólo si" en la definición es muy importante. Por ejemplo, establece que dos elementos en P son comparables siempre y cuando sus imágenes vía la biyección son comparables en Q. Además, dice cómo deben compararse dos elementos en P si sabemos cómo se comparan sus imágenes en Q. En el caso en que se tengan conjuntos linealmente ordenados, el siguiente teorema nos asegura que el "sólo si" puede suprimirse en la Definición 4.123.

Teorema 4.124 *Sean $(P, \leq)$ y $(Q \preceq)$ conjuntos linealmente ordenados y sea $h : P \to Q$ una biyección tal que $h(p_1) \preceq h(p_2)$ siempre que $p_1 \leq p_2$. Entonces h es un isomorfismo entre $(P, \leq)$ y $(Q, \preceq)$.*

Demostración:

Debemos mostrar que si $p_1, p_2 \in P$ con $p_1 \neq p_2$ son tales que $h(p_1) \preceq h(p_2)$, entonces $p_1 \leq p_2$. Si suponemos que p_1 no es menor que p_2, como $\leq$ es un orden lineal en P, entonces $p_1 = p_2$, o bien $p_2 < p_1$. Hemos supuesto que $p_1 \neq p_2$, por lo tanto, $p_2 < p_1$. Por hipótesis esto implica que $h(p_2) \prec h(p_1)$, lo cual es una contradicción. ■

Proposición 4.125 *(a) Si $(P, \leq)$ y $(Q, \preceq)$ son conjuntos ordenados isomorfos y $\leq$ es un orden lineal, entonces $\preceq$ también es un orden lineal.*

(b) La función identidad es un isomorfismo de $(P, \leq)$ en sí mismo.

(c) Si h es un isomorfismo entre $(P, \leq)$ y $(Q, \preceq)$, entonces h^{-1} es un isomorfismo entre $(Q, \preceq)$ y $(P \leq)$.

(d) Si f es un isomorfismo entre $(P, \leq)$ y $(Q, \preceq)$ y g es un isomorfismo entre $(Q, \preceq)$ y $(T, \ll)$, entonces $g \circ f$ es un isomorfismo entre $(P, \leq)$ y $(T, \ll)$.

La parte *(a)* de la proposición anterior puede interpretarse diciendo que si tenemos dos conjuntos ordenados isomorfos y uno de ellos tiene la propiedad de ser lineal, entonces el otro también la tiene. Otras propiedades que se preservan con isomorfismos pueden encontrarse en los ejercicios. Las partes *(b), (c)* y *(d)* nos dicen que la propiedad "... es isomorfo a ..." es reflexiva, simétrica y transitiva. Así, desde el punto de vista de los conjuntos ordenados es indistinto manipular un conjunto ordenado o un isomorfo a él.

Un ejemplo típico de un conjunto ordenado (parcialmente) es el conjunto potencia ordenado por la contención. El siguiente resultado muestra que cualquier conjunto ordenado es básicamente de este tipo.

Teorema 4.126 *Todo conjunto ordenado $(A, \leq)$ es isomorfo a una familia indizada de subconjuntos de A, parcialmente ordenada por la contención.*

DEMOSTRACIÓN:

Para cada $a \in A$, definamos $S_a = \{x \in A : x \leq a\}$. Entonces la función $h : A \to \{S_a\}_{a \in A}$ definida por $h(a) = S_a$ verifica la afirmación. En efecto, claramente h es una biyección; además, $a_1 \leq a_2$ si y sólo si $a_1 \in S_{a_2}$. Por la transitividad, $S_{a_1} \subseteq S_{a_2}$. Luego, $a_1 \leq a_2$ si y sólo si $S_{a_1} \subseteq S_{a_2}$. ■

Los conjuntos S_a definidos en la demostración anterior son usados con frecuencia.

Definición 4.127 Si $(A, \leq)$ es un conjunto parcialmente ordenado, el *segmento inicial determinado por $a \in A$* es el conjunto

$$U_a = \{x \in A : x < a\}.$$

El siguiente tipo de conjunto totalmente ordenado es muy importante.

Definición 4.128 Un conjunto parcialmente ordenado $(W, \leq)$ se llama *bien ordenado* si cada subconjunto no vacío $B \subseteq W$ tiene elemento mínimo. En este caso al orden $\leq$ se le llama *buen orden.*

Cualquier conjunto bien ordenado $(W, \leq)$ es totalmente ordenado, puesto que cada subconjunto $\{a, b\} \subseteq W$ tiene elemento mínimo. Más aún, el orden inducido (ver Ejercicio 4.5.9) a un subconjunto de un conjunto bien ordenado es un buen orden en el subconjunto. Es costumbre referirse al mínimo elemento de un subconjunto B como primer elemento.

Ejemplo 4.129 $\emptyset$ es un conjunto bien ordenado.

Ejemplo 4.130 Sea $(A, \leq)$ un conjunto linealmente ordenado. Cualquier conjunto $B = \{a_1, a_2, \ldots, a_n\} \subseteq A$ es un conjunto bien ordenado con el orden inducido por $\leq$ en B.

Ejemplo 4.131 El ordenamiento por inclusión en $\mathcal{P}(X)$ no es un buen orden en cualquier X con más de un elemento.

Ejemplo 4.132 Sean $(W, \leq)$ un conjunto bien ordenado y $q \notin W$. En $W \cup \{q\}$ definimos un buen orden que coincida con $\leq$ en W de la manera siguiente: $q \preceq q$, para cada $w \in W$, $w \preceq q$, y para $w_1, w_2 \in W$, $w_1 \preceq w_2$ si y sólo si $w_1 \leq w_2$. Decimos que $W \cup \{q\}$ se forma adjuntando un punto a W como último elemento. Demostraremos que $\preceq$ es, en efecto, un buen orden. Para cada $B \subseteq W \cup \{q\}$ no vacío, o bien $B = \{q\}$ o $B \cap W \neq \emptyset$. En el último caso, el primer elemento de $B \cap W$ en $(W, \leq)$ es el primer elemento de B en $(W \cup \{q\}, \preceq)$. Por lo tanto, $(W \cup \{q\}, \preceq)$ es un conjunto bien ordenado.

Cada elemento w en un conjunto bien ordenado $(W, \leq)$ que tiene un sucesor en W, tiene un *sucesor inmediato*; esto es, podemos encontrar $s \in W$ con $s \neq w$ que satisfaga $w \leq s$ y tal que ningún $c \in W \setminus \{s\}$ satisface $w \leq c \leq s$. En efecto, necesitamos tan sólo elegir $s = \min\{x \in W : w < x\}$, lo cual es posible dado que $\{x \in W : w < x\} \neq \emptyset$ y $(W, \leq)$ es bien ordenado. Sin embargo, aún cuando un elemento w en un conjunto bien ordenado tenga un predecesor, no necesariamente tiene un predecesor inmediato. Por ejemplo, si $W \neq \emptyset$ es un conjunto bien ordenado y no acotado superiormente, entonces adjuntando un punto q como último elemento de W a la manera del Ejemplo 4.132, q no tiene un predecesor inmediato.

Veamos ahora algunos otros tipos importantes de funciones definidas entre conjuntos ordenados.

Definición 4.133 Sean $(A, \leq)$ y $(B, \preceq)$ conjuntos linealmente ordenados y $f : A \to B$ una función.

(a) f se llama *creciente* si $a_1, a_2 \in A$ con $a_1 \leq a_2$ implica $f(a_1) \preceq f(a_2)$.

(b) f se llama *decreciente* si $a_1, a_2 \in A$ con $a_1 \leq a_2$ implica $f(a_1) \succeq f(a_2)$.

A una función creciente también se le dice *función que preserva el orden* y a una función decreciente también se le dice *función que invierte el orden.*

Lema 4.134 *Si $(W, \leq)$ es un conjunto bien ordenado y $f : W \to W$ es una función creciente e inyectiva, entonces $f(x) \geq x$ para cada $x \in W$.*

Demostración:

Supongamos que $X = \{x \in W : f(x) < x\}$ es no vacío y sea $w = \min X$. Sea $f(w) = z$. Como $w \in X$, $z < w$, y siendo f creciente se cumple que $f(z) < z$, lo cual contradice la elección de w. ■

Corolario 4.135 *El único isomorfismo de un conjunto bien ordenado en sí mismo es la identidad.*

DEMOSTRACIÓN:

Por el Lema 4.134, si $(W, \leq)$ es un conjunto bien ordenado y

$$f : W \to W$$

es un isomorfismo, entonces $f(x) \geq x$ y $f^{-1}(x) \geq x$ para todo $x \in W$. Esto implica que $f(x) = x$ para todo $x \in W$; o sea, $f = Id_W$. ■

Corolario 4.136 *Si dos conjuntos bien ordenados son isomorfos, entonces el isomorfismo es único.*

Lema 4.137 *Ningún conjunto bien ordenado es isomorfo a un segmento inicial de sí mismo.*

DEMOSTRACIÓN:

Supongamos que $(W, \leq)$ es un conjunto bien ordenado que es isomorfo a uno de sus segmentos iniciales, y sea f el isomorfismo entre ellos. Entonces para alguna $u \in W$,

$$f(W) = \{x \in W : x < u\},$$

luego $f(u) < u$, que contradice el Lema 4.134. ■

Finalmente, veamos el resultado más relevante sobre conjuntos bien ordenados que presentamos en esta sección.

Teorema 4.138 *Si $(W_1, \leq_1)$ y $(W_2, \leq_2)$ son dos conjuntos bien ordenados, entonces exactamente uno de los siguientes tres casos se cumple:*

(a) $(W_1, \leq_1)$ es isomorfo a $(W_2, \leq_2)$;
(b) $(W_1, \leq_1)$ es isomorfo a un segmento inicial de $(W_2, \leq_2)$;
(c) $(W_2, \leq_2)$ es isomorfo a un segmento inicial de $(W_1, \leq_1)$.

DEMOSTRACIÓN:

Para $u_i \in W_i$ $(i = 1, 2)$, sea $W_i(u_i) = \{x \in W_i : x < u_i\}$ el segmento inicial de W_i determinado por u_i. Sea

$$f = \{(x, y) \in W_1 \times W_2 : W_1(x) \text{ es isomorfo a } W_2(y)\}.$$

Usando el Lema 4.137, es fácil ver que f es inyectiva. Si h es un isomorfismo entre $W_1(x)$ y $W_2(y)$ y $x' < x$, entonces $W_1(x')$ y $W_2(h(x'))$ son isomorfos; de aquí se sigue que f es creciente.

Si $dom\, f = W_1$ y $ran\, f = W_2$, entonces ocurre el caso *(a)*.

Si $y_1 <_2 y_2$ y $y_2 \in ran\, f$, entonces $y_1 \in ran\, f$. Así, si $ran\, f \neq W_2$ y $y_0 = \min W_2 \setminus ran\, f$, tenemos que $ran\, f = W_2(y_0)$. Necesariamente, $dom\, f = W_1$, de otro modo tenemos $(x_0, y_0) \in f$, donde $x_0 = \min W_1 \setminus dom\, f$. Así, el caso *(b)* se cumple.

Similarmente, si $dom\, f \neq W_1$, entonces se tiene el caso *(c)*.

Por el Lema 4.137, los tres casos considerados son mutuamente excluyentes. ■

Intuitivamente este resultado puede interpretarse diciendo que los conjuntos bien ordenados pueden compararse por su "longitud", un hecho que será de mucha importancia en lo sucesivo.

Ejercicios 4.5

1. Sea R una relación reflexiva y transitiva. Defina $\approx$ en A por $a \approx b$ si y sólo si (aRb) y (bRa).

   (a) Muestre que $\approx$ es una relación de equivalencia en A.

   (b) Si $\ll$ se define por $[a] \ll [b]$ si y sólo si aRb; muestre que $(A/\approx, \ll)$ es un conjunto ordenado.

2. Muestre que $R \subseteq A \times A$ es reflexiva y transitiva si y sólo si $Id_A \subseteq R$ y $R \circ R = R$.

3. Sea $\mathbf{R}^{\mathbf{R}}$ el conjunto de todas las funciones de los números reales en sí mismos. Pruebe que definiendo $f \preceq g$ si y sólo si $\forall x \in \mathbf{R}$, $f(x) \leq g(x)$, $(\mathbf{R}^{\mathbf{R}}, \preceq)$ es un conjunto ordenado.

4. Pruebe el Teorema 4.103.

5. (a) Sea R un orden en A. Sean S el correspondiente orden estricto en A y R^* el orden correspondiente a S. Muestre que $R = R^*$.

   (b) Sea S un orden estricto en A, sea R su correspondiente orden en A, y sea S^* el orden estricto correspondiente a R. Entonces $S = S^*$. Ver Teorema 4.103.

6. Formule las definiciones de elementos incomparable, maximal, minimal, máximo, mínimo, supremo e ínfimo en términos de órdenes estrictos.

7. Pruebe que el Axioma de Fundación es equivalente a que todo conjunto no vacío A tiene un elemento $\in_A$-minimal.

8. Sea R un orden en A. Pruebe que R^{-1} es también un orden en A (se llama *dual de* R), y para $B \subseteq A$ se cumple que

   (a) a es el mínimo elemento de B en R^{-1} si y sólo si a es el máximo elemento de B en R.

   (b) Similarmente para minimal y maximal, y supremo e ínfimo.

9. Sean R un orden en A y $B \subseteq A$. Muestre que $R \cap (B \times B)$ es un orden en B. Este orden se llama *orden inducido por R en B*.

10. Muestre que el diagrama correspondiente al conjunto

$$\{1, 2, 3, 5, 6, 10, 15, 30\}$$

    con el orden inducido por el dual de la divisibilidad en los enteros, es idéntico al último presentado en la figura (4.5.1).

11. Dar ejemplos de un conjunto ordenado finito (A, R) y un subconjunto $B \subseteq A$ tales que:

    (a) B tiene un elemento máximo.

    (b) B no tiene elemento mínimo.

    (c) B no tiene máximo, pero B tiene supremo.

    (d) B no tiene supremo.

12. Sean $(A, \leq)$ y $(B, \preceq)$ dos conjuntos ordenados con $A \cap B = \emptyset$. Defina $\ll$ como sigue:

$$\begin{array}{rll} x \ll y & \text{si y sólo si} & x, y \in A \text{ y } x \leq y \\ & \text{o} & x, y \in B \text{ y } x \preceq y \\ & \text{o} & x \in A \text{ y } y \in B. \end{array}$$

    Muestre que $\ll$ es un orden en $A \cup B$ y que $\ll$ restringido a A es $\leq$, y $\ll$ restringido a B es $\preceq$. Intuitivamente $\ll$ pone a todo elemento de B después de todo elemento de A y coincide con los ordenes originales en A y B; esta es la razón de que al orden $\ll$ se le llama *orden de yuxtaposición*.

13. Verifique el Ejemplo 4.112.

14. Sean $(A, \leq)$ y $(B, \preceq)$ dos conjuntos ordenados. Muestre que $\ll$ es un orden parcial en $A \times B$, donde $\ll$ se define como $(a_1, b_1) \ll (a_2, b_2)$ si y sólo si $a_1 \leq a_2$ y $b_1 \preceq b_2$. El conjunto ordenado $(A \times B, \ll)$ se llama *producto (cartesiano)* de los conjuntos ordenados $(A, \leq)$ y $(B, \preceq)$.

15. Sea $\mathcal{F}$ la familia de todas las funciones desde X hacia T (ver Ejercicio 4.2.19). Defina la relación $\leq$ en $\mathcal{F}$ por

$$f \leq g \quad \text{si y sólo si} \quad f \subseteq g.$$

    (a) Pruebe que $\leq$ es un orden.

    (b) Sea $\mathcal{A} \neq \emptyset$, $\mathcal{A} \subseteq \mathcal{F}$. Pruebe que $\sup \mathcal{A}$ existe si y sólo si $\mathcal{A}$ es una familia de funciones compatibles. Pruebe además que si $\sup \mathcal{A}$ existe, entonces $\sup \mathcal{A} = \bigcup \mathcal{A}$.

16. Sean $A \neq \emptyset$ y $Pt(A)$ el conjunto de todas las particiones de A. Defina una relación $\leq$ en $Pt(A)$ por: $\mathcal{S}_1 \leq \mathcal{S}_2$ si y sólo si para todo $B \in \mathcal{S}_1$, existe $C \in \mathcal{S}_2$ tal que $B \subseteq C$.

    Cuando $\mathcal{S}_1 \leq \mathcal{S}_2$ se dice que la partición $\mathcal{S}_1$ es un *refinamiento* de $\mathcal{S}$.

    (a) Muestre que $\leq$ es un orden.

    (b) Sean $\mathcal{S}_1, \mathcal{S}_2 \in Pt(A)$. Muestre que $\{\mathcal{S}_1, \mathcal{S}_2\}$ tiene ínfimo. (Sugerencia: defina $\mathcal{S} = \{B \cap C : B \in \mathcal{S}_1,\ C \in \mathcal{S}_2\}$).
    ¿Cómo es la relación de equivalencia $E_{\mathcal{S}}$ con respecto a las relaciones de equivalencia $E_{\mathcal{S}_1}$ y $E_{\mathcal{S}_2}$?

    (c) Sea $\mathcal{T} \subseteq Pt(A)$, $\mathcal{T} \neq \emptyset$. Muestre que $\inf \mathcal{T}$ existe.

    (d) Sea $\mathcal{T} \subseteq Pt(A)$, $\mathcal{T} \neq \emptyset$. Muestre que $\sup \mathcal{T}$ existe. (Sugerencia: sea $\mathcal{T}'$ el conjunto de todas las particiones $\mathcal{S}$ con la propiedad que cualquier partición de $\mathcal{T}$ es un refinamiento de $\mathcal{S}$. Muestre que $\mathcal{T}' \neq \emptyset$ y que $\sup \mathcal{T} = \sup \mathcal{T}'$.)

17. Pruebe el Teorema 4.118.

18. Pruebe la segunda parte del Teorema 4.120.

19. Muestre que en una cadena los conceptos de elemento máximo y elemento maximal coinciden, y muestre lo mismo para elemento mínimo y elemento minimal.

20. Un conjunto (parcialmente) ordenado es una *retícula* si para cada $a, b \in A$, el conjunto $\{a, b\}$ tiene supremo e ínfimo.

(a) Muestre que $(\mathbf{R}^{\mathbf{R}}, \preceq)$ como en el problema 3 es una retícula.

(b) Muestre que $(\mathcal{P}(A), \subseteq)$ es una retícula.

(c) Muestre que $(\mathbf{Z}, |)$ es una retícula.

(d) Muestre que $(Pt(A), \leq)$ es una retícula.

21. Sea $(X, \leq)$ un conjunto totalmente ordenado. Una *cortadura de* X es un par de subconjuntos A, B que satisfacen: *(i)* $X = A \cup B$, *(ii)* $A \cap B = \emptyset$ y *(iii)* $a \in A \ \wedge \ b \in B \Rightarrow a \leq b$. Si A, B y A', B' son dos cortaduras de X, pruebe que $A \subseteq A'$ o que $A' \subseteq A$.

22. Sea $(A, \leq)$ un conjunto ordenado con la propiedad de que todo subconjunto no vacío con una cota superior tiene supremo. Pruebe que A tiene la propiedad de que cualquier subconjunto de A no vacío con una cota inferior tiene ínfimo. A las propiedades anteriores se les llama propiedad de la *mínima cota superior* y propiedad de la *máxima cota inferior*.

23. Si $(A, \leq)$ es un conjunto ordenado y $a, b \in A$ con $a \leq b$, se define el intervalo cerrado de extremos a, b como el conjunto

$$[a, b] = \{x \in A : a \leq x \text{ y } x \leq b\}.$$

Pruebe que el conjunto de intervalos cerrados ordenados por la inclusión es isomorfo a un subconjunto del producto de $(A, \leq)$ y su dual $(A, \leq^{-1})$.

24. Pruebe la Proposición 4.125.

25. Muestre que h es un isomorfismo entre $(A, \leq)$ y $(B, \preceq)$ si y sólo si h y h^{-1} preservan el orden.

26. Pruebe por medio de un ejemplo que si $(A, \leq)$ y $(B, \preceq)$ son conjuntos ordenados y $f : A \to B$ es una biyección que preserva el orden, entonces $f^{-1} : B \to A$ no necesariamente preserva el orden.

27. Muestre que si A es un conjunto finito, entonces todo orden total en A es un buen orden.

28. Muestre que un conjunto bien ordenado $(W, \leq)$ tiene la propiedad de la mínima cota superior.

29. Sean A, B conjuntos bien ordenados. Demuestre que los órdenes lexicográfico vertical y lexicográfico horizontal en $A \times B$ son también buenos órdenes.

30. Pruebe el Corolario 4.136.

31. Sea $(A, \leq)$ un conjunto bien ordenado. Muestre que no existen una sucesiones $\{a_n \in A : n \in \mathbf{N}\}$ tales que $a_{n+1} \leq a_n$ y $a_n \neq a_{n+1}$ para toda $n \in \mathbf{N}$.

4.6 Sobre Clases

Considere la siguiente forma de asignación: A cada par ordenado de conjuntos (A, B) le podemos asociar de manera única el conjunto $A \cup B$. Parece claro que esta regla de asociación permite establecer una función. No obstante, esta "función" tendría como dominio el producto cartesiano de la clase de todos los conjuntos con sí misma (*clase* como en la Convención 2.5); por lo que no sería, propiamente hablando, una función por no ser un conjunto. Sin embargo, la regla de asociación cumple la propiedad importante de las funciones, a saber,

$$(a, b) \in f \quad \text{y} \quad (a, c) \in f \quad \text{implica} \quad b = c.$$

Por esta razón, no es mala idea considerar a esta asignación como una "función" entre clases. Pensada como "función entre clases" la asignación que estamos considerando quedaría expresada como:

$$\mathbf{Un} : \mathbf{V} \times \mathbf{V} \to \mathbf{V}$$

donde $\mathbf{V}$ es la clase de todos los conjuntos y $\mathbf{Un}(A, B) = A \cup B$. De esta manera, la unión de conjuntos puede ser pensada como una función. La ventaja es que podemos aprovechar nuestro conocimiento sobre funciones legítimas para intuir propiedades generales que, como operación, posea la unión de conjuntos.

Ahora bien, pensar en $\mathbf{Un}$ como función requiere que primero tengamos claro qué entendemos por $\mathbf{V} \times \mathbf{V}$.

Si $\mathbf{K}_1$ y $\mathbf{K}_2$ son dos clases, de manera completamente análoga a las definiciones para conjuntos, es posible "definir" la unión, intersección, complemento y producto cartesiano de $\mathbf{K}_1$ y $\mathbf{K}_2$. Por ejemplo, la unión de $\mathbf{K}_1$ y $\mathbf{K}_2$ está dada por

$$\mathbf{K}_1 \cup \mathbf{K}_2 = \langle x : (x \in \mathbf{K}_1) \ \vee \ (x \in \mathbf{K}_2) \rangle$$

y el producto cartesiano de $\mathbf{K}_1$ y $\mathbf{K}_2$ está dado por

$$\mathbf{K}_1 \times \mathbf{K}_2 = \langle (x, y) : x \in \mathbf{K}_1, \ y \in \mathbf{K}_2 \rangle .$$

Remarcamos que escribimos "*definir*" porque en realidad no estamos haciendo una definición en nuestra teoría, sino una convención fuera de ella.

Habiendo establecido las operaciones elementales entre clases, extender conceptos como los de función, orden y relación de equivalencia a clases ya no debe presentar dificultades.

Además de que la extensión de conceptos a clases puede llegar a ser fructífera para intuir propiedades generales sobre conjuntos, esta extensión nos permitirá mayores posibilidades para expresarnos. Por ejemplo, podemos decir que la relación "conjuntos ordenados isomorfos" es de equivalencia en la clase de todos los conjuntos ordenados (que no es un conjunto).

En lo sucesivo emplearemos estas convenciones sobre clases; pero, *para no tener repercusión en el formalismo de nuestra teoría, las expresiones que involucren clases deben ser pensadas únicamente como abreviaciones para expresiones que no involucren clases.* En el ejemplo anterior sobre conjuntos ordenados isomorfos, formalmente se debe decir: en cualquier familia de conjuntos ordenados, la relación de isomorfismo es una relación de equivalencia.

También, con el afán de evitar posibles confusiones, distinguiremos las funciones, órdenes y relaciones de equivalencia entre clases, de los respectivos conceptos para conjuntos escribiendo la palabra *clase* entre paréntesis antes del concepto correspondiente. Así escribiremos (clase) función, (clase) orden parcial, etc.

5

Los Números Naturales

5.1 Introducción

Para desarrollar las matemáticas dentro de la Teoría de Conjuntos, es necesario definir a los números naturales.

Para una persona medianamente instruida, el punto de partida obvio de la matemática son los números naturales

$$1, 2, 3, 4, \ldots \text{ etc.}$$

Probablemente, sólo a una persona con algunos conocimientos de matemáticas se le ocurriría empezar por el 0 y no por el 1:

$$0, 1, 2, 3, \ldots, n, n+1, \ldots.$$

El hombre requirió un alto grado de civilización para tomar así a los números naturales como punto de partida. Debe haber pasado largo tiempo para que alguien descubriera que una pareja de águilas y un par de piedras eran ejemplos del número 2. El grado de abstracción que ello implica no es fácil de adquirir. En la actualidad los números naturales parecen representar lo más sencillo y conocido de la matemática. Sin embargo, conocido no significa bien comprendido. Hay pocas personas que disponen de una definición clara de lo que es un número natural.

Nosotros intuitivamente conocemos a los números naturales. El propósito de este capítulo es suplir esa idea intuitiva por una definición rigurosa de lo que son los números naturales, así como mostrar sus propiedades elementales.

Podemos intentar definir un número, por ejemplo, 2 como "2 es una abstracción que es común a todos los conjuntos que tienen dos elementos". Esta "definición" es circular: usa la palabra *dos* para definir al número dos. Una observación no trivial consiste en que podemos reformular esta "definición" con base a un ejemplo específico: 2 es la cualidad común a todos los conjuntos que tienen el mismo número de elementos que $\{\emptyset, \{\emptyset\}\}$. Esta nueva definición se refiere a *número* en la frase "el número de elementos".

La siguiente observación no trivial es que podemos definir la proposición "los conjuntos A y B tienen el mismo número de elementos" sin ningún conocimiento previo de la noción de número.

Definición 5.1 Los conjuntos A y B son *equipotentes* (*tienen la misma cardinalidad* o *la misma potencia*) si hay una función biyectiva f con domino A y rango B.

La equipotencia tiene propiedades interesantes.

Teorema 5.2 *(a) A es equipotente a sí mismo, para todo conjunto A.*

(b) Si A es equipotente a B, entonces B es equipotente a A.

(c) Si A es equipotente a B y B es equipotente a C, entonces A es equipotente a C.

Demostración:

(a) Id_A es una función biyectiva de A en sí mismo (ver Ejemplo 4.46).

(b) Si $f : A \to B$ es una función biyectiva, entonces $f^{-1} : B \to A$ también es una función biyectiva.

(c) Si $f : A \to B$ y $g : B \to C$ son funciones biyectivas, entonces $g \circ f : A \to C$ es una función biyectiva. ■

Aparentemente estamos ya en posición de crear una buena definición para el número 2. Con la noción de equipotencia podemos reformular la definición de 2 como sigue: 2 es aquello común a todos los conjuntos equipotentes a $\{\emptyset, \{\emptyset\}\}$. Falta precisar qué es "aquello común a todos los conjuntos equipotentes a un conjunto dado A".

Observemos que el Teorema 5.2, asegura que la propiedad "A es equipotente a B" es reflexiva, simétrica y transitiva; es decir, tiene los atributos de una relación de equivalencia, salvo por un detalle que más adelante el lector será capaz de deducir con facilidad.

En la Sección 4.4 vimos que hay al menos dos maneras de poder representar, en Teoría de Conjuntos, lo "que es común a todos los elementos mutuamente equivalentes". Una de estas maneras es usar clases de equivalencia, otra es usar el conjunto de representantes. Desgraciadamente ambas maneras están lejos de nuestro alcance. Por ejemplo, se puede mostrar que si $A \neq \emptyset$, *el conjunto de todos los conjuntos equipotentes a A, no existe*; es decir, las "clases de equivalencia" de la relación de equipotencia no son conjuntos. Este es el mismo hecho que nos impide aplicar la segunda forma. Al parecer, si tuviéramos en estos momentos establecido al Axioma de Elección podríamos aplicar éste a las clases de equivalencia de la relación de equipotencia y obtener de este modo

un conjunto de representantes para tal relación; el gran problema es que el Axioma de Elección (como todos los Axiomas de nuestro sistema **ZFC**) es aplicable únicamente a objetos de la Teoría de Conjuntos; o sea, a conjuntos.

Aunque pudiera parecer que las consideraciones anteriores están lejos de ayudarnos a dar una definición de número natural, eso no es cierto. En primer lugar, nos han ayudado a tener claro qué es lo que pretendemos; por ejemplo, queremos que 2 caracterice a toda la multitud de conjuntos que tienen la misma cardinalidad que $\{\emptyset, \{\emptyset\}\}$. En segundo lugar, nos han revelado que es imposible caracterizar a toda esa multitud de conjuntos. Sin embargo, quizá pudiéramos realizar esa caracterización procediendo a la inversa, definiendo explícitamente cada número natural como un representante conveniente para tal multitud de conjuntos; después de todo, eso es lo que pretendíamos hacer al tomar a $\{\emptyset, \{\emptyset\}\}$ como parámetro para definir a 2. La forma de realizar esa definición explícita se sustenta en la idea intuitiva de que los números naturales se van generando uno a partir de otro. También, es aquí donde sacaremos provecho de empezar la serie de los números naturales con 0 en vez de 1.

Empecemos por elegir un representante para el 0. La opción de un conjunto sin elementos es trivial, puesto que existe un único conjunto vacuo, $\emptyset$. Definamos 0 como el conjunto $\emptyset$. Busquemos ahora un buen representante para los conjuntos que tienen sólo un elemento. Puesto que tenemos ya definido un objeto en particular, a saber 0, una opción natural es definir

$$1 = \{0\} = \{\emptyset\}.$$

Luego consideremos los conjuntos de dos elementos. Como tenemos definidos 0, 1 y $0 \neq 1$ podemos definir

$$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}.$$

El proceso puede continuar así:

$$\begin{aligned}
3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \\
5 &= \{0, 1, 2, 3, 4\}, \text{ etc.}
\end{aligned}$$

La idea es simplemente definir un número natural n como el conjunto de todos los números naturales más pequeños: $\{0, 1, \ldots, n-1\}$; de este modo, n es un conjunto particular con n elementos.

Desgraciadamente esta idea tiene una deficiencia fundamental. Tenemos definidos a 0, 1, 2, 3, 4, 5 y uno puede fácilmente definir 17 o 324; pero no

proporciona un enunciado que diga qué es un número natural en general. Necesitamos una proposición de la forma: "Un conjunto n es un número natural si ... ". No podemos únicamente definir un número natural como un conjunto n tal que sus elementos son todos los número naturales más pequeños que él, puesto que tal definición involucra el concepto que se desea definir. Pero sí podemos usar esto como una "guía" hacia la abstracción de las propiedades que hacen a n un número natural.

Analicemos la forma de construcción del número 5. Primero note que los números naturales previamente definidos (0, 1, 2, 3 y 4) son subconjuntos del número natural 5; esto es, sus elementos son subconjuntos de él mismo. Esta no es una propiedad común a todos los conjuntos; por ejemplo, el conjunto $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ tiene como elemento al conjunto $\{\emptyset, \{\emptyset\}\}$, pero este conjunto no es subconjunto de él.

Definición 5.3 Decimos que un conjunto x es *transitivo* si para todo $y \in x$, y es un subconjunto de x; o sea, $y \subseteq x$.

El argumento del párrafo anterior a la Definición 5.3 sugiere que todos los números naturales son conjuntos transitivos. Por otro lado, no todos los conjuntos transitivos son números naturales: el conjunto $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ es transitivo y tiene tres elementos pero no es igual al número 3.

Para ver qué propiedades distinguen a los números naturales de los conjuntos transitivos, regresemos a la idea de un número natural n como el conjunto de todos los números más pequeños que n; esto significa que m es más pequeño que n si y sólo si $m \in n$. La relación $\in_n$ (pertenencia restringida al conjunto n) es un orden lineal estricto. Observe que el conjunto transitivo $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ no tiene esta propiedad porque $\emptyset \notin \{\{\emptyset\}\}$ y $\{\{\emptyset\}\} \notin \emptyset$.

Finalmente, el ordenamiento lineal $\in_n$ tiene otra propiedad: Sea X un subconjunto no vacío de n, intuitivamente se puede tomar uno a uno los elementos de n y verificar si son elementos de X, y hallar así el elemento máximo y mínimo de X. Estas consideraciones motivan la siguiente definición de número natural.

Definición 5.4 Un conjunto x es un *número natural* si:

(a) x es transitivo,

(b) $\in_x$ es un orden lineal estricto en x,

(c) todo subconjunto no vacío de x tiene elementos mínimo y máximo en el orden $\in_x$.

Mientras las consideraciones anteriores a la definición muestran que intuitivamente los números naturales tienen las propiedades *(a), (b)* y *(c)*, el

recíproco no es obvio. Para convencernos de su validez, en la siguiente sección derivaremos algunas de las propiedades básicas de los números naturales a partir de nuestra definición.

La idea de definir a los números naturales a partir de la Teoría de Conjuntos se debe a Frege en [F_3]; de hecho, B. Russell [R_4] afirma que Frege fue el primero que dio una definición satisfactoria de número, pero que apenas despertó atención y su definición de número permaneció prácticamente ignorada hasta que fue redescubierta por él en 1901. Sin embargo, la manera en que hemos definido a los números naturales es muy distinta de la idea original de Frege. Nuestra presentación, que hoy en día es más o menos corriente, fue iniciada por Von Neumann en [N_1].

Ejercicios 5.1

1. Sea $A \neq \emptyset$. Demuestre que no existe un conjunto $\mathcal{S}$ que contenga a todos los conjuntos equipotentes a A. (Sugerencia: muestre que $\bigcup \mathcal{S}$ sería la clase de todos los conjuntos.)

2. Pruebe que un conjunto X es transitivo si y sólo si $X \subseteq \mathcal{P}(X)$.

3. Pruebe que un conjunto X es transitivo si y sólo si $\bigcup X \subseteq X$.

4. ¿Son los siguientes conjuntos transitivos?

   (a) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$,
   (b) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$,
   (c) $\{\emptyset, \{\{\emptyset\}\}\}$.

5. ¿Cuáles de los conjuntos del ejercicio anterior son números naturales?

6. Pruebe o dé contraejemplos para las siguientes proposiciones.

   (a) Si X y Y son transitivos, entonces $X \cup Y$ es transitivo.
   (b) Si X y Y son transitivos, entonces $X \cap Y$ es transitivo.
   (c) Si $X \in Y$ y Y es transitivo, entonces X es transitivo.
   (d) Si X es transitivo, entonces $\bigcap X$ es transitivo.
   (e) Si $X \subseteq Y$ y Y es transitivo, entonces X es transitivo.

(f) Si Y es transitivo y $\mathcal{S} \subseteq \mathcal{P}(Y)$, entonces $Y \cup \bigcup \mathcal{S}$ es transitivo.

7. Pruebe que si X es un conjunto transitivo y todo elemento de X es un conjunto transitivo, entonces $\bigcup X$ y $\bigcap X$ son conjuntos transitivos.

5.2 Propiedades de los Números Naturales

Iniciamos con dos lemas de utilidad.

Lema 5.5 *Todo elemento de un número natural es un número natural.*

Demostración:

Sea n un número natural, y sea $x \in n$. Mostraremos que x cumple las propiedades (a), (b) y (c) de la Definición 5.4. En primer lugar hay que probar que x es transitivo. Supóngase que u y v son tales que $u \in v$ y $v \in x$. Entonces $v \in n$ y también $u \in n$. Así $u, v, x \in n$ y $u \in v$, $v \in x$. Usando el hecho que $\in_n$ ordena linealmente a n, se concluye que $u \in x$; con esto concluimos que x es transitivo.

En segundo lugar, mostraremos que $\in_x$ es un orden lineal estricto en x y que todo subconjunto no vacío de x tiene elementos mínimo y máximo en el orden $\in_x$. Por la transitividad de n, se tiene que $x \subseteq n$ y por lo tanto, la relación $\in_x$ es la restricción de la relación $\in_n$ a x, es decir, $\in_x = \in_n \cap (x \times x)$. Así, las correspondientes propiedades de $\in_x$ se siguen de las mismas de $\in_n$. ■

El siguiente lema se sigue del Axioma de Fundación, pero aquí exhibiremos una demostración que no utiliza dicho axioma.

Lema 5.6 *Si n es un número natural entonces $n \notin n$. Si m y n son números naturales, entonces $m \notin n$ o $n \notin m$.*

Demostración:

Si $n \in n$ entonces el conjunto ordenado $(n, \in_n)$ tiene un elemento $x = n$ tal que $x \in x$, que contradice la suposición de que $\in_n$ es un orden lineal estricto.

Para la segunda proposición, si $n \in m$ y $m \in n$, entonces por la transitividad de n, tenemos que $n \in n$, una contradicción. ■

Usaremos ahora estos lemas para dar una caracterización de los números naturales más simple. Si observamos nuevamente la construcción de los primeros números, definimos $2 = \{0, 1\}$; para obtener 3 adjuntamos a 2 un tercer

elemento, a saber,

$$3 = 2 \cup \{2\} = \{0, 1\} \cup \{2\}\,.$$

Similarmente

$$4 = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\}$$
$$5 = 4 \cup \{4\} = \{0, 1, 2, 3\} \cup \{4\}$$
etc.

Dado un número natural n, obtenemos el "siguiente" número adjuntando un elemento más a n, a saber, n mismo. Este procedimiento empieza en 0, pues de hecho, 0 es el primer número natural.

Definición 5.7 El *sucesor* de un conjunto x es el conjunto $S(x) = x \cup \{x\}$.

La noción de sucesor la emplearemos posteriormente para definir la adición de números naturales. Obsérvese que $S(x) = x \cup \{x\}$ define una (clase) función, es decir, una "función" en el sentido de la Sección 4.6.

Teorema 5.8 *(a)* 0 *es un número natural.*
(b) Si x *es un número natural, entonces* $S(x)$ *es un número natural.*

Demostración:

(a) No hay nada que probar, pues $0 = \emptyset$ cumple la definición.

(b) Sea n un número natural, y sea $x = S(n) = n \cup \{n\}$. Primero mostraremos que x es transitivo. Sea $u \in x$, entonces $u \in n$ o $u = n$. Si $u \in n$, tenemos que $u \subseteq n$, ya que n es transitivo, por lo que $u \subseteq x$, porque $n \subseteq x$. Si $u = n$ es claro que $u \subseteq x$.

Luego note que para $u, v \in x$, $u \in_x v$ si y sólo si ($u, v \in n$ y $u \in_n v$) o ($u \in n$ y $v = n$). Observe que el Lema 5.6 excluye las posibilidades $u \in v$ y $u = n$, $v \in n$ o $u = n$ y $v = n$.

Debemos verificar que $\in_x$ es un orden lineal estricto en x. Sabemos que $\in_x$ es un orden estricto en x. Sean u, $v \in x = S(n)$, entonces o bien $u, v \in n$, y en este caso $u \in v$ o $u = v$ o $v \in u$, puesto que $\in_n$ es un orden lineal estricto; o $u \in n = v$ o $v \in n = u$ o $u = n = v$. En cada caso u y v son comparables.

Por último, sea $X \subseteq S(n)$ con $X \neq \emptyset$. Si $X \cap n \neq \emptyset$, el elemento mínimo del conjunto $X \cap n$ también lo es de X; el elemento máximo de X es el mismo que el de $X \cap n$ en el orden $\in_n$, o bien es n. Si $X \cap n = \emptyset$, n es el elemento máximo y mínimo de X. ■

Definición 5.9 Llamamos a un conjunto A *inductivo* si:
(a) $0 \in A$,
(b) $x \in A$ implica $S(x) \in A$.

Con la definición anterior, el Teorema 5.8 asegura que el conjunto de los números naturales es inductivo. Hay una única dificultad con esta formulación: no hemos probado que el conjunto de los números naturales exista. Hay una buena razón para esto, los axiomas tratados hasta ahora no implican la existencia de conjuntos de una infinidad de objetos. Pero la posibilidad de colecciones infinitas de objetos en una entidad singular es la esencia de la Teoría de Conjuntos. Por tanto, extendemos nuestro sistema axiomático.

Axioma 8 (de Infinitud) *Existe un conjunto inductivo.*

Intuitivamente, el conjunto de los números naturales es uno de ellos. Más aún, todo número natural puede ser obtenido a partir de 0 aplicando suficientes veces la (clase) función sucesor. En otras palabras, si un conjunto A contiene a 0 y al sucesor de cada uno de sus elementos, entonces A contiene a 0, $1 = S(0)$, $2 = S(1)$, ..., y así contiene a todo número natural. Esto motiva el siguiente resultado básico.

Teorema 5.10 *Todo conjunto inductivo contiene a todos los números naturales.*

Demostración:

Sea A un conjunto inductivo y supongamos que x es un número natural que no pertenece al conjunto A. Entonces $S(x)$ es un número natural y $x \in S(x) \setminus A$. Sea y el elemento mínimo del conjunto no vacío $S(x) \setminus A$ ordenado por $\in_{S(x)}$. Note que $y \subseteq S(x)$, ya que $S(x)$ es transitivo. Además, $y \subseteq A$ puesto que si existe $u \in y \setminus A$, entonces y no es el elemento mínimo de $S(x) \setminus A$. Por el Lema 5.5, y es un número natural. Si $y = \emptyset$, entonces $y \in A$, que es una contradicción. Por lo tanto, $y \neq \emptyset$. Sea z el elemento máximo de y en el orden $\in_y$. Entonces $z \in A$, más aún, puesto que $z \in y$, y y es transitivo $z \subseteq y$, consecuentemente $z \cup \{z\} = S(z) \subseteq y$; si $u \in y \setminus S(z)$ entonces $u \notin z$ y $u \neq z$. Como y es un natural, $\in_y$ es un orden lineal estricto, entonces $z \in u$ que contradice la elección de z como el máximo elemento de y, es decir, $y \setminus S(z) = \emptyset$; así $S(z) \supseteq y$. Por lo tanto, $y = S(z) \in A$, nuevamente una contradicción. ■

Corolario 5.11 *El conjunto* $\mathbf{N}$ *de los números naturales existe.*

Demostración:

Sea A un conjunto inductivo.

$$\mathbf{N} = \{x : x \text{ es un número natural}\} = \{x \in A : x \text{ es un número natural}\}$$

es un conjunto por el Axioma Esquema de Comprensión. ■

El Teorema 5.10 simplemente dice que $\mathbf{N}$ es el mínimo conjunto inductivo en el (clase) orden $\subseteq$ de la clase de todos los conjuntos inductivos, es decir, $\mathbf{N} \subseteq A$ para cualquier conjunto inductivo A.

Una consecuencia inmediata del Teorema 5.10 es el bien conocido Principio de Inducción Matemática.

Teorema 5.12 (Principo de Inducción) *Sea* $\mathbf{P}(x)$ *una propiedad (posiblemente con parámetros). Supongamos que:*

(a) $\mathbf{P}(0)$,

(b) $\forall n \in \mathbf{N}$, $\mathbf{P}(n) \Rightarrow \mathbf{P}(S(n))$.

Entonces $\mathbf{P}(n)$ *para todos los números naturales* n.

Demostración:

Las suposiciones *(a)* y *(b)* simplemente dicen que el conjunto

$$A = \{n \in \mathbf{N} : \mathbf{P}(n)\}$$

es inductivo, por lo que $\mathbf{N} \subseteq A$. ■

A continuación definiremos un orden en el conjunto $\mathbf{N}$. La idea de definir cada número natural como el conjunto de todos los números naturales más pequeños, sugiere inmediatamente la Definición 5.13.

Definición 5.13 Para cualesquiera $m, n \in \mathbf{N}$, definimos $m \leq n$ si y sólo *si* $m \in n$ *o* $m = n$.

Teorema 5.14 $(\mathbf{N}, \leq)$ *es un conjunto bien ordenado.*

Demostración:

1 Reflexividad. Obvia.

2 Antisimetría. Se sigue del Lema 5.6.

3 Transitividad. Si $k \leq m$ y $m \leq n$, entonces tenemos que $k \in m$ o $k = m$ y $m \in n$ o $m = n$; si ambas igualdades se verifican no hay nada que probar. Si $k \in m$ y $m = n$, entonces $k \leq n$. Similarmente si $k = m$ y $m \in n$. Finalmente si $k \in m$ y $m \in n$, como n es transitivo $k \in n$, así $k \leq n$.

4 Buen Orden. Primero estableceremos que $\leq$ ordena linealmente a $\mathbf{N}$. Usualmente decimos que m y n son comparables si $m < n$, $m = n$ o $n < m$. Decimos que $n \in \mathbf{N}$ es comparable si n es comparable con todo $m \in \mathbf{N}$. Es suficiente con demostrar por inducción que cualquier $n \in \mathbf{N}$ es comparable.

i) 0 es comparable. Probaremos por inducción sobre m que 0 es comparable con todo m. Claramente 0 es comparable con 0. Asumamos que 0 es comparable con m. Entonces, o bien $0 \in m$ o $0 = m$. En cada caso, $0 \in m \cup \{m\} = S(m)$. Así, 0 es comparable con $S(m)$. La conclusión se sigue del Principio de Inducción.

ii) Supongamos que n es comparable. Nuevamente por inducción sobre m probaremos que $S(n)$ es comparable con m, para todo $m \in \mathbf{N}$. Sabemos que $S(n)$ es comparable con 0 por *i)*. Supongamos que $S(n)$ es comparable con m, entonces $S(n) \in m$, $S(n) = m$ o $m \in S(n)$. En los primeros dos casos $S(n) \in m \cup \{m\} = S(m)$; en el último caso $m = n$ o $m \in n$. Si $m = n$, $S(n) = S(m)$. Si $m \in n$, $S(m)$ y n son comparables por hipótesis de inducción (n es comparable). Como $m \in n$, es imposible tener $n \in m$ o $m = n$, es decir, $n \in S(m)$ no puede ocurrir. Por lo tanto, $S(m) = n$ o $S(m) \in n$; en cualquier caso $S(m) \in S(n)$. Se concluye que $S(n)$ es comparable, y que cualquier número natural lo es.

Ahora sea $M \in \mathbf{N}$ con $M \neq \emptyset$. Tomemos algún $m \in M$ y consideremos $S(m) \cap M$; éste es un conjunto no vacío de números naturales en $S(m)$. Si k es el elemento mínimo de $S(m) \cap M$ en el orden $\in_{S(m)}$, entonces k es también el primer elemento de M en el orden $\leq$, porque de lo contrario existiría $k' \in M$ tal que $k' \leq k$ y $k' \neq k$, entonces $k' \in k$, por lo que $k' \in S(m)$ y así $k' \in S(m) \cap M$, que contradice la elección de k. ■

Ejercicios 5.2

1. Pruebe que $S(x)$ es una (clase) función de la clase de todos los conjuntos en la clase de todos los conjuntos.

2. Pruebe que si $n \in \mathbf{N}$, entonces no existe un $k \in \mathbf{N}$ tal que $n < k < S(n)$.

3. Pruebe:

   (a) $S(x) = S(y)$ implica $x = y$.
   (b) $\bigcup S(x) = x$.

4. Demuestre que para cualquier $n \in \mathbf{N}$, $n \neq 0$, existe $k \in \mathbf{N}$ tal que $n = S(k)$.

5. Demuestre que para cualquier $n \in \mathbf{N} \setminus \{0, 1\}$, existe $k \in \mathbf{N}$ tal que $n = S(S(k))$.

6. Pruebe que si $m, n \in \mathbf{N}$ y $m \subset n$, entonces $m < n$.

7. Pruebe que si $X \subseteq \mathbf{N}$, entonces $(X, X^2 \cap \leq)$ es un conjunto bien ordenado.

8. Dar un conjunto inductivo $A \neq \mathbf{N}$.

9. (a) Pruebe por inducción que si $a \in n$ y $n \in \mathbf{N}$, entonces $a \in \mathbf{N}$. Concluya que $\mathbf{N}$ es un conjunto transitivo.
   (b) Pruebe que si $S(a) \in \mathbf{N}$, entonces $a \in \mathbf{N}$.

10. Pruebe que $\mathbf{N}$ es equipotente a algún subconjunto propio de $\mathbf{N}$.

11. Demuestre el Principio de Inducción Finita: Sea $\mathbf{P}(x)$ una propiedad. Supóngase que $k \in \mathbf{N}$ y *(a)* $\mathbf{P}(0)$ se verifica, *(b)* para todo $n < k$, $\mathbf{P}(n)$ implica $\mathbf{P}(S(n))$. Entonces $\mathbf{P}(n)$ se cumple para todo $n < k$.

12. (a) Sea $K \subseteq \mathbf{N}$ no vacío, demuéstrese que $\bigcap K \in \mathbf{N} \cap K$.
    (b) Use lo anterior para probar que $(\mathbf{N}, \leq)$ es bien ordenado.

13. Deduzca el Teorema 5.14 a partir del Axioma de Fundación (ver Ejercicio 4.5.7).

5.3 El Teorema de Recursión

En la siguiente sección nuestro objetivo será definir la adición y multiplicación de números naturales. Para hacer más sencillo esto, introduciremos un importante método de definir funciones en $\mathbf{N}$.

Empezaremos con dos ejemplos informales:

1) La función $s : \mathbf{N} \to \mathbf{N}$ definida por:

$$\begin{aligned} &s(0) = 1, \\ &s(n+1) = n^2, \text{ para todo } n \in \mathbf{N}. \end{aligned}$$

2) La función $f : \mathbf{N} \to \mathbf{N}$ definida por:

$$\begin{aligned} &f(0) = 1 \\ &f(n+1) = f(n) \cdot (n+1), \text{ para todo } n \in \mathbf{N}. \end{aligned}$$

Las dos funciones, a pesar de tener similitudes superficiales, difieren en un aspecto crucial. La definición de s dice explícitamente cómo calcular $s(x)$ para

cualquier $x \in \mathbf{N}$. Más precisamente, ésta nos capacita para formular una propiedad $\mathbf{P}$ tal que

$$s(x) = y \text{ si y sólo si } \mathbf{P}(x, y);$$

a saber: $x = 0$ y $y = 1$, o para algún $n \in \mathbf{N}$, $x = n+1$ y $y = n^2$. La existencia y unicidad de una función s que satisfaga *1)* se sigue inmediatamente de nuestros axiomas:

$$s = \{(x, y) \in \mathbf{N} \times \mathbf{N} : \mathbf{P}(x, y)\}.$$

En contraste, las instrucciones provistas por la definición de f nos dicen cómo calcular $f(x)$ teniendo el valor de f para algún número más pequeño (a saber, $x - 1$). No es inmediatamente obvio cómo formular una propiedad $\mathbf{P}$ que no involucre la función f en su definición y tal que

$$f(x) = y \text{ si y sólo si } \mathbf{P}(x, y).$$

La definición *2)* proporciona condiciones que debe satisfacer la función f: f es una función de $\mathbf{N}$ en $\mathbf{N}$ que satisface la condición inicial: $f(0) = 1$, y la condición recursiva: para todo $n \in \mathbf{N}$, $f(n + 1) = f(n) \cdot (n + 1)$.

Este tipo de definiciones recursivas son ampliamente usadas en matemáticas. Sin embargo, una definición recursiva está justificada sólo si es posible mostrar que existe alguna función que satisfaga las condiciones requeridas, y que no existen dos o más de tales funciones.

Teorema 5.15 (de Recursión) *Para cualquier conjunto A, cualquier $a \in A$, y cualquier función $g : A \times \mathbf{N} \to A$, existe una única función $f : \mathbf{N} \to A$ tal que*

(a) $f(0) = a$,
(b) $f(S(n)) = g(f(n), n)$, *para todo* $n \in \mathbf{N}$.

En el ejemplo *2)*, tenemos $A = \mathbf{N}$, $a = 1$ y $g(u, v) = u \cdot (v+1)$. El elemento a es el "valor inicial" de f. El papel que desempeña g es proveer de instrucciones para calcular $f(S(n))$, asumiendo que $f(n)$ ha sido calculado.

La demostración del Teorema de Recursión consiste en derivar una definición explícita de f. Considerando nuevamente el ejemplo *2)*, $f(n)$ es el factorial de n, y una definición explícita de f puede ser escrita como:

$$f(0) = 1 \text{ y}$$
$$f(m) = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (m-1) \cdot m, \text{ si } m \in \mathbf{N} \setminus \{0\}.$$

El problema es hacer "$\cdots$" preciso. Esto puede ser resuelto si decimos que f es el resultado del cálculo

$$\begin{array}{l} 1 \\ 1 \cdot 1 \\ [1 \cdot 1] \cdot 2 \\ [1 \cdot 1 \cdot 2] \cdot 3 \\ \vdots \\ [1 \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (m-1)] \cdot m \end{array}$$

de longitud m. Un cálculo de longitud m basado en g puede ser descrito por una función t tal que $dom\, t = m+1$, $t(0) = 1$ y $t(k+1) = t(k) \cdot (k+1) = g(t(k), k)$ para todo $0 < k < m$. La definición rigurosa y explícita de f es entonces: $f(0) = 1$ y $f(m) = t(m)$, donde t es un cálculo de longitud m basado en g. El problema de mostrar la existencia y unicidad de f se reduce al problema de mostrar que hay precisamente un cálculo de longitud m basado en g para cada $m \in \mathbf{N}$ $(m \neq 0)$.

Procedemos ahora con la demostración formal del Teorema de Recursión que está entre los métodos más importantes de la Teoría de Conjuntos.

Demostración:

La *existencia* de f. Una función $t : S(m) \to A$ se llama *cálculo de longitud m basado en g*, si $t(0) = a$, y para todo k tal que $0 < k < m$, $t(S(k)) = g(t(k), k)$. Note que $t \subseteq \mathbf{N} \times A$.

Sea

$$\mathcal{F} = \{t \subseteq \mathbf{N} \times A : t \text{ es un cálculo de longitud } m,\ m \in \mathbf{N}\}$$

y sea $f = \bigcup \mathcal{F}$. Mostraremos que f es una función. Para esto es suficiente mostrar que el sistema de funciones $\mathcal{F}$ es compatible (ver Teorema 4.55). Sean $t_1, t_2 \in \mathcal{F}$; supongamos que $dom\, t_1 = n_1 \in \mathbf{N}$ y $dom\, t_2 = n_2 \in \mathbf{N}$. Sin pérdida de generalidad supongamos $n_1 \leq n_2$, entonces $n_1 \subseteq n_2$, y basta con demostrar que $t_1(k) = t_2(k)$ para todo $k < n_1$. Haremos esto por inducción: $t_1(0) = t_2(0) = a$; luego sea k tal que $S(k) < n_1$ y asumamos que $t_1(k) = t_2(k)$, entonces

$$t_1(S(k)) = g(t_1(k), k) = g(t_2(k), k) = t_2(S(k)).$$

Así, $t_1(k) = t_2(k)$ para todo $k < n_1$.

Ahora mostraremos que $dom\, f = \mathbf{N}$ y $ran\, f \subseteq A$. Es inmediato que $dom\, f \subseteq \mathbf{N}$ y que $ran\, f \subseteq A$. Para mostrar que $dom\, f = \mathbf{N}$, basta con probar que para cada $n \in \mathbf{N}$ hay un cálculo de longitud n. Usaremos el Principio de Inducción. Claramente $t_0 = \{(0, a)\}$ es un cálculo de longitud 0. Asumamos que t es

un cálculo de longitud n. Entonces la siguiente función t^+ en $S(S(n))$ es un cálculo de longitud $S(n)$:

$$t^+(k) = t(k), \text{ si } k \leq n$$
$$t^+(S(n)) = g(t(n), n).$$

Por lo tanto, para cada $n \in \mathbf{N}$ hay un cálculo de longitud n, por lo que concluimos que cada $n \in \mathbf{N}$ está en el dominio de algún cálculo $t \in \mathcal{F}$, así

$$\mathbf{N} \subseteq \bigcup \{dom\, t : t \in \mathcal{F}\} = dom\, f.$$

Finalmente mostraremos que f satisface las condiciones *(a)* y *(b)*. Claramente $f(0) = a$ puesto que $t(0) = a$ para todo $t \in \mathcal{F}$. Para mostrar que $f(S(n)) = g(f(n), n)$, para cada $n \in \mathbf{N}$, sea t un cálculo de longitud $S(n)$, entonces $t(k) = f(k)$, para todo $k \in dom\, t$, y así

$$f(S(n)) = t(S(n)) = g(t(n), n) = g(f(n), n).$$

La existencia de la función f con las propiedades requeridas por el teorema está demostrada.

La *unicidad*. Sea $h : \mathbf{N} \to A$ tal que

(a') $h(0) = a$,
(b') $h(S(n)) = g(h(n), n)$, para todo $n \in \mathbf{N}$.

Mostraremos que $f(n) = h(n)$, para todo $n \in \mathbf{N}$ usando nuevamente inducción. Claramente $f(0) = h(0)$. Si $f(n) = h(n)$, entonces

$$f(S(n)) = g(f(n), n) = g(h(n), n) = h(S(n)),$$

por lo tanto, $f = h$. ■

En ocasiones se usa el Teorema de Recursión para definir funciones de dos variables, es decir, funciones en $\mathbf{N} \times \mathbf{N}$. Este resultado es comúnmente formulado como una versión "paramétrica" del Teorema de Recursión.

Teorema 5.16 (Recursión Paramétrica) *Sean A y P conjuntos, y sean $a : P \to A$ y $g : P \times A \times \mathbf{N} \to A$ funciones. Entonces existe una única función $f : P \times N \to A$ tal que*

(a) $f(p, 0) = a(p)$ para todo $p \in P$,
(b) $f(p, S(n)) = g(p, f(p, n), n)$ para todo $n \in \mathbf{N}$ y $p \in P$.

La demostración del Teorema 5.16 es una versión "paramétrica" de la prueba del Teorema de Recursión. Alternativamente, ésta puede ser deducida directamente de este último.

En algunas definiciones recursivas, el valor de $f(S(n))$ depende no solamente de $f(n)$, sino también de $f(k)$ para algún $k \leq n$. Un ejemplo típico es la sucesión de Fibonacci:

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ ...$$

Aquí $f(0) = 1$, $f(1) = 1$, y $f(n+2) = f(n+1) + f(n)$ para $n \geq 0$.

El siguiente teorema formaliza esta forma de construcción recursiva de manera un poco más general. También puede deducirse del Teorema de Recursión.

Teorema 5.17 *Sea A un conjunto, sea $\mathcal{S} = \bigcup_{n\in\mathbf{N}}(A^n)$ el conjunto de todas las funciones con dominio un número natural y valores en A, y sea $g : \mathcal{S} \to A$ una función. Entonces existe una única función $f : \mathbf{N} \to A$ tal que*

$$f(n) = g(f\mid_n) \text{ para todo } n \in \mathbf{N}.$$

Note que, en particular, $f(0) = g(f\mid_0) = g(\emptyset)$.

Otra versión del Teorema de Recursión se encuentra en los ejercicios.

Concluimos esta sección con un teorema que da una caracterización del orden de los números naturales. La prueba ilustra un empleo típico del Teorema de Recursión en la Teoría de Conjuntos. Llamamos *acotado* a un subconjunto B de conjunto ordenado $(A, \preceq)$ si tiene cota inferior y cota superior.

Teorema 5.18 *Sea $(A, \preceq)$ un conjunto no vacío linealmente ordenado con las siguientes propiedades:*

(a) Para todo $p \in A$ existe $q \in A$ tal que $p \prec q$,

(b) todo subconjunto no vacío de A tiene un elemento mínimo en el orden $\preceq$,

(c) todo subconjunto acotado no vacío de A tiene un elemento máximo en el orden $\preceq$.

Entonces $(A, \preceq)$ es isomorfo a $(\mathbf{N}, \leq)$.

Demostración:

Construyamos un isomorfismo $f : \mathbf{N} \to A$ empleando el Teorema de Recursión. Sea a el elemento mínimo de A y sea

$$g(x, n) = \min\{y \in A : x \prec y\}$$

para todo $n \in \mathbf{N}$. Entonces $a \in A$ y g es una función de $A \times \mathbf{N}$ en A. Observe que $g(x, n)$ está definido para cualquier $x \in A$, por las hipótesis *(a)*

y *(b)*; además $g(x,n)$ no depende de n. El Teorema de Recursión garantiza la existencia y unicidad de una función $f : \mathbf{N} \to A$ tal que

(i) $f(0) = a = \min A$,

(ii) $f(S(n)) = g(f(n), n)$ (el elemento mínimo de A mayor que $f(n)$).

Es obvio que $f(n) \prec f(S(n))$ para cada $n \in \mathbf{N}$. Por inducción, se tiene que $f(m) \prec f(n)$ siempre que $m < n$. Consecuentemente, f es una función inyectiva. Resta probar que $f(\mathbf{N}) = A$.

Supóngase que $A \setminus f(N) \neq \emptyset$ y sea $p = \min A \setminus f(\mathbf{N})$. El conjunto

$$B = \{q \in A : q \prec p\}$$

es acotado (p es una cota superior) y no vacío (de otro modo, p sería el mínimo elemento de A, pero entonces $p = f(0)$). Sea q el elemento máximo de B (éste existe por la hipótesis *(c)*). Como $q \prec p$, tenemos que $q = f(m)$ para algún $m \in \mathbf{N}$. Sin embargo, es fácil ver que p es el mínimo elemento de A mayor que q. Por lo tanto, $p = f(S(m))$ por la condición recursiva *(ii)*. Consecuentemente $p \in f(\mathbf{N})$, que es una contradicción. ■

Ejercicios 5.3

1. Demuestre el Teorema 5.17 de modo análogo al Teorema de Recursión.

2. Demuestre el Teorema 5.17 usando el Teorema de Recursión. (Sugerencia: defina $G : \mathcal{S} \times \mathbf{N} \to \mathcal{S}$ por $G(x,n) = x \cup \{(n, g(x))\}$. Use entonces el Teorema de Recursión para encontrar $F : \mathbf{N} \to \mathcal{S}$ tal que $F(0) = \emptyset$ y $F(S(n)) = G(F(n), n)$. Finalmente tome $f = \bigcup F(\mathbf{N})$.)

3. Demuestre la versión "paramétrica" del Teorema de Recursión usando el Teorema 5.15. (Sugerencia: defina $F : \mathbf{N} \to A^P$ por recursión: $F(0) = a$ y $F(S(n)) = G(F(n), n)$, donde $G : A^P \times \mathbf{N} \to A^P$ está definida por $G(x,n)(p) = g(x(p), n, p)$ $(x \in A^P,\ n \in \mathbf{N})$ Sea entonces $f(m,p) = F(m)(p)$.)

4. Demuestre la siguiente versión del Teorema de Recursión: Sea g una función en $A \times \mathbf{N}$ y sea $a \in A$. Entonces hay una única función f tal que
   (a) $f(0) = a$,
   (b) $f(S(n)) = g(f(n), n)$ para todo n tal que $S(n) \in dom\, f$,
   (c) o bien $dom\, f = \mathbf{N}$ o $dom\, f = S(k)$ donde k es el elemento máximo de $\{k \in \mathbf{N} : g(f(k), k) \notin A\}$.

5. Sean A un conjunto y $f : A \to A$ una función. Defina f^n por

$$f^0 = Id_A,$$
$$f^{n+1} = f^n \circ f \text{ para todo } n \in \mathbf{N}.$$

Pruebe que para cada $n \in \mathbf{N}$, f^n es un elemento unívocamente determinado de A^A.

6. Use el ejercicio anterior para demostrar que para cada $X \subseteq \mathbf{N}$ existe una función inyectiva f tal que $ran\, f = X$ y $dom\, f = \mathbf{N}$ o $dom\, f \in \mathbf{N}$.

7. Sea $a \in A$ y sea $h : A \to A$ una función inyectiva tal que $a \notin ran\, h$. Demuestre que existe una función inyectiva $f : \mathbf{N} \to A$. (Sugerencia: considere $g(x, n) = h(x)$, use el Teorema de Recursión y el Principio de Inducción.)

8. Sea A un conjunto y sea $f : A \to B$ una función inyectiva, donde $B \subseteq A$. Pruebe que A tiene un subconjunto equipotente a $\mathbf{N}$. (Sugerencia: use el ejercicio anterior.)

9. Sea $f : \mathbf{N} \to A$ una función donde A es linealmente ordenado por $\preceq$, y suponga que $f(n) \preceq f(S(n))$ para todo $n \in \mathbf{N}$. Pruebe que $m \leq n$ implica $f(m) \preceq f(n)$ para todo $m, n \in \mathbf{N}$. (Sugerencia: use inducción sobre m.)

5.4 Aritmética de los Números Naturales

Ahora discutiremos brevemente las operaciones aritméticas en los números naturales. Nuestro principal interés en esta sección es mostrar que estas operaciones pueden ser satisfactoriamente definidas. El tópico da una oportunidad para aplicar el Teorema de Recursión y el Principio de Inducción.

Una *operación binaria* en un conjunto A es una función

$$* : A \times A \to A.$$

El valor (resultado) de $*$ en (x, y) se denota usualmente como $x * y$, en lugar de $*(x, y)$.

Teorema 5.19 *Hay una única operación binaria* $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ *tal que:*
(a) $0 + m = m$, *para todo* $m \in \mathbf{N}$,
(b) $S(m) + n = S(m + n)$, *para todo* $m, n \in \mathbf{N}$.
Esta función es llamada adición o suma de números naturales.

DEMOSTRACIÓN:

Sea n un elemento fijo de $\mathbf{N}$. Definamos $g : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ por $g(x, y) = S(y)$. Por el Teorema 5.15 existe exactamente una función $f_n : \mathbf{N} \to \mathbf{N}$ donde $f_n(0) = n$ y $f_n(S(m)) = g(m, f_n(m)) = S(f_n(m))$. Ahora definamos

$$f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$$

por $f(m, n) = f_n(m)$. Claramente esta función satisface 5.19(a) y 5.19(b). Para probar su unicidad, sea h cualquier función de $\mathbf{N} \times \mathbf{N}$ en $\mathbf{N}$ que también satisfaga 5.19(a) y 5.19(b). Para cada $n \in \mathbf{N}$, defina $h_n : \mathbf{N} \to \mathbf{N}$ por $h_n(0) = h(0, n)$ y $h_n(m) = h(m, n)$. Entonces $h_n(0) = h(0, n) = n$ y

$$h_n(S(m)) = h(S(m), n) = S(h(m, n)) = S(h_n(m)).$$

Nuevamente, por el Teorema de Recursión 5.15 se sigue que $f_n = h_n$ para todo $n \in \mathbf{N}$. Así, para $m, n \in \mathbf{N}$,

$$f(m, n) = f_n(m) = h_n(m) = h(m, n).$$

Por lo tanto, $f = h$. Haciendo $+ = f$, se tiene la conclusión. ■

Haciendo $m = 0$ en 5.19(b), se implica que $S(0) + n = S(0 + n)$, pero por 5.19(a) $S(0 + n) = S(n)$, y como $S(0) = 1$, tenemos

$$n + 1 = S(n).$$

Llegamos así a una notación más intuitiva del sucesor de n, $n + 1$. Así, las propiedades de la adición pueden ser reformuladas como:

5.19(a') $0 + m = m$

5.19(b') $(m + 1) + n = (m + n) + 1$.

También, se puede formular el Teorema de Recursión de una manera más palpable. Primero, definimos una *sucesión* como una función con dominio $\mathbf{N}$. Una sucesión cuyo dominio es algún $n \in \mathbf{N}$ es llamada *sucesión finita* de *longitud* n y es denotada como:

$$(a_i)_{i<n} \quad \text{o} \quad (a_i)_{i=0}^{n-1},$$

su rango es denotado por

$$\{a_0, a_1, \ldots a_{n-1}\} \quad \text{o} \quad \{a_i\}_{i=0}^{n-1}$$

A las sucesiones las denotamos por

$$(a_n)_{n\in\mathbf{N}} \quad \text{o} \quad (a_n)_{n=0}^{\infty}\,.$$

La notación simplemente especifica una función con un dominio apropiado, cuyo valor en i es a_i. Del mismo modo usamos la notación

$$\{a_n : n \in \mathbf{N}\}\,, \quad \{a_n\}_{n\in\mathbf{N}}\,, \quad \text{etc.}$$

para el rango de la sucesión $(a_n)_{n=0}^{\infty}$.

Remarcaremos que un conjunto se llama *finito* si es el rango de alguna sucesión finita.

Usando esta nueva terminología, podemos reformular el *Teorema de Recursión*. Sean $a \in A$ y g una función de $A \times \mathbf{N}$ en A. Entonces existe una única sucesión $(a_n)_{n=0}^{\infty}$ tal que

$$\begin{aligned} &a_0 = a \\ &a_{n+1} = g(a_n, n) \text{ para todo } n \in \mathbf{N}. \end{aligned}$$

El lector seguramente reformulará las otras versiones del Teorema de Recursión por sí mismo.

En el siguiente Teorema se enuncian las principales propiedades de la adición

Teorema 5.20 *La adición en* $\mathbf{N}$ *tiene las siguientes propiedades.*

A_1. *Asociatividad. Para todo* $m, n, p \in \mathbf{N}$,

$$m + (n + p) = (m + n) + p.$$

A_2. *Conmutatividad. Para todo* $m, n \in \mathbf{N}$,

$$m + n = n + m.$$

A_3. *Ley de Cancelación. Para todo* $m, n, p \in \mathbf{N}$,

$$m + p = n + p \quad \Rightarrow \quad m = n.$$

A_4. *Para todo* $m, n \in \mathbf{N}$,

$$m \leq n \quad \Leftrightarrow \quad \exists p \in \mathbf{N},\ m + p = n.$$

A_5. *Para todo* $m, n, p \in \mathbf{N}$,

$$m < n \quad \Leftrightarrow \quad m + p < n + p.$$

A_6. *Para todo* $m, n \in \mathbf{N}$,

$$m + n = 0 \quad \Leftrightarrow \quad m = 0 \ \text{ y } \ n = 0.$$

DEMOSTRACIÓN:

A_1. Sean $n, p \in \mathbf{N}$ fijos y sea

$$M = \{m \in \mathbf{N} : m + (n + p) = (m + n) + p\}.$$

Entonces $0 \in M$ puesto que $0 + (n + p) = (0 + n) + p$.

Supongamos que $m \in M$, entonces

$$\begin{aligned}(m + 1) + (n + p) &= [m + (n + p)] + 1 \\ &= [(m + n) + p] + 1 \\ &= [(m + n) + 1] + p \\ &= [(m + 1) + n] + p,\end{aligned}$$

así que $m + 1 \in M$. Por lo tanto, $M = \mathbf{N}$ y la prueba de A_1 está completa.

A_2. Primero, para $m \in \mathbf{N}$ fijo probaremos que

$$S(n) + m = n + S(m), \tag{5.4.1}$$

para todo $n \in \mathbf{N}$. Procediendo por inducción, es cierto para 0 pues $S(0)+m = S(0 + m) = 0 + S(m)$. Luego suponiendo que es cierto para $n \in \mathbf{N}$, dado que

$$\begin{aligned}S(S(n)) + m &= S(S(n) + m) \\ &= S(n + S(m)) \\ &= S(n) + S(m),\end{aligned}$$

por 5.19(b), la ecuación (5.4.1) es cierta para todo $n \in \mathbf{N}$.

Por otro lado, para $n \in \mathbf{N}$ fijo, sea

$$M_n = \{m \in \mathbf{N} : m + n = n + m\}.$$

Si $m \in M_n$, entonces $S(m)+n = S(m+n) = S(n+m) = S(n)+m = n+S(m)$ por (5.4.1), esto implica que $S(m) \in M_n$.

Finalmente, es claro que $0 \in M_0$, y dado que $S(m) \in M_0$ si $m \in M_0$, entonces $M_0 = \mathbf{N}$. También como $0 \in M_n$, y puesto que $m \in M_n$ implica $S(m) \in M_n$, entonces, por el principio de inducción, $M_n = \mathbf{N}$ para cada $n \in \mathbf{N}$. Así, A_2 esta probada.

A_3. Probaremos equivalentemente que si $m, n \in \mathbf{N}$ con $m \neq n$, entonces $m + p \neq n + p$ para todo $p \in \mathbf{N}$. Claramente $0 \in \{p \in \mathbf{N} : m + p \neq n + p\}$; luego supongamos que p es un miembro de este conjunto, entonces $m + p \neq n + p$, por lo cual se sigue que $S(m + p) \neq S(n + p)$, que es equivalente a $S(m)+p \neq S(n)+p$; o bien aplicando la ecuación (5.4.1), $m+S(p) \neq n+S(p)$.

O sea, $S(p)$ también es miembro del conjunto. Esto concluye la prueba de que $m + p \neq m + p$ implica $m \neq n$.

A_4. Sean $m, n \in \mathbf{N}$ con $m \leq n$. Entonces

$$A = \{x \in \mathbf{N} : x + m \geq n\} \neq \emptyset$$

(en efecto, se puede mostrar por inducción que $m + n \geq n$ para cualesquiera $m, n \in \mathbf{N}$). Consecuentemente A tiene un elemento mínimo p por el Teorema 5.14. Así tenemos que $p + m = n$ o bien $p + m > n$. Supóngase que $m + p > n$, entonces claramente $p \neq 0$ y por lo tanto, p es el sucesor de algún natural q; entonces $S(q) + m = S(q + m) > n$, que implica que $q + m \geq n$ puesto que $q < S(q) = p$; esto contradice la elección de p. Por lo tanto, $m + p = n$.

A_5. Si $m < n$, entonces $m + d = n$ para algún $d \in \mathbf{N}$ con $d \neq 0$ (usando A_4). Por lo tanto, $p + n = p + (d + m) = (p + d) + m = (d + p) + m = d + (p + m)$. Así, por A_4, $p + m \leq p + n$, y puesto que $d \neq 0$, la desigualdad estricta se sigue.

Similarmente se prueba el recíproco.

A_6. Probaremos, equivalentemente, que si $m \neq 0$ o $n \neq 0$, entonces $m + n \neq 0$. Supongamos que $m \neq 0$, entonces existe un $p \in \mathbf{N}$ tal que $m = S(p)$. Por lo tanto, $m + n = S(p + n)$, y consecuentemente $m + n \neq 0$. Así, si m o n son diferentes de cero, también lo es $m + n$. ■

Ahora se definirá la multiplicación.

Teorema 5.21 *Hay una única operación $\cdot$ en $\mathbf{N}$ tal que*

(a) $\cdot(0, n) = 0$ *para todo* $n \in \mathbf{N}$,

(b) $\cdot(m + 1, n) = \cdot(m, n) + n$.

Escribiremos $m \cdot n$ o simplemente mn en lugar de $\cdot(m, n)$. A esta operación se le llama multiplicación.

Demostración:

Sea $n \in \mathbf{N}$ fijo y sea $g : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ dada por $g(x, y) = y + n$. Por el Teorema 5.15, existe exactamente una función $f_n : \mathbf{N} \to \mathbf{N}$ donde $f_n(0) = 0$ y $f_n(S(m)) = g(m, f_n(m)) = f_n(m) + n$.

Ahora definimos $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ por $f(m, n) = f_n(m)$, para $m, n \in \mathbf{N}$. Claramente esta función satisface *(a)* y *(b)*. Su unicidad puede ser inferida de la unicidad de las funciones f_n para cada n. ■

También para el caso de la multiplicación establecemos algunas de sus propiedades más elementales.

Teorema 5.22 *La multiplicación en* $\mathbf{N}$ *tiene las siguientes propiedades.*

M_1. *Asociatividad. Para todo* $m, n, p \in \mathbf{N}$,

$$m(np) = (mn)p.$$

M_2. *Conmutatividad. Para todo* $m, n \in \mathbf{N}$,

$$mn = nm.$$

M_3. *Ley de Cancelación. Para todo* $m, n, p \in \mathbf{N}$, $p \neq 0$,

$$pm = pn \quad \Rightarrow \quad m = n.$$

M_4. *Distribución sobre la adición. Para todo* $m, n, p \in \mathbf{N}$,

$$m(n + p) = mn + mp.$$

M_5. *Para todo* $m, n, p \in \mathbf{N}$, $p \neq 0$,

$$m < n \quad \Leftrightarrow \quad pm < pn.$$

M_6. *Para todo* $m, n \in \mathbf{N}$,

$$mn = 0 \quad \Rightarrow \quad m = 0 \text{ o } n = 0.$$

Demostración:

Es conveniente probar estas propiedades en el orden M_4, M_2, M_1, M_6, M_3, M_5.

M_4. Para n y p fijos considérese

$$A = \{m \in \mathbf{N} : m(n + p) = mn + mp\}.$$

Claramente $0 \in A$, y si $m \in A$, entonces $S(m) \in A$ puesto que

$$\begin{aligned} S(m)(n + p) &= m(n + p) + (n + p) \\ &= (mn + mp) + (n + p) \\ &= (mn + n) + (mp + p) \\ &= S(m)n + S(m)p. \end{aligned}$$

Con lo cual, $A = \mathbf{N}$. Esto establece M_4.

M_2. Se puede probar por inducción que para todo $n \in \mathbf{N}$, $n \cdot 0 = 0$ y $n \cdot S(0) = n$. Supongamos estos preliminares y sea $n \in \mathbf{N}$ fijo. Considérese

$\{m \in \mathbf{N} : mn = nm\}$. Este conjunto contiene a 0 puesto que $0 \cdot n = 0 = n \cdot 0$. Supongamos que contiene a m, entonces

$$\begin{aligned} S(m) \cdot n &= mn + n \\ &= nm + n \\ &= nm + n \cdot S(0) \\ &= n(m + S(0)) \\ &= n(S(0) + m) \\ &= n \cdot S(m); \end{aligned}$$

así, $S(m)$ es un elemento del conjunto. Por el Principio de Inducción, M_2 está probada.

M_1. Para $n, p \in \mathbf{N}$ fijos considere $\{m \in \mathbf{N} : m(np) = (mn)p\}$. Este conjunto contiene a 0, y si contiene a m, entonces contiene a $S(m)$ puesto que $S(m) \cdot (np) = m(np) + (np) = (mn)p + (np) = (mn + n)p = (S(m) \cdot n)p$.

M_6. Asumamos que $mn = 0$ y $m \neq 0$. Entonces $m = S(p)$ para algún $p \in \mathbf{N}$. Como $0 = mn = S(p) \cdot n = pn + n$, entonces, por A_6, $n = 0$.

M_3. Supongamos que $pm = pn$ y $p \neq 0$. Como $\leq$ es un orden lineal en $\mathbf{N}$, entonces $m \leq n$ o $n \leq m$. Sin pérdida de generalidad supongamos que $m \leq n$, entonces por A_4, $n = d + m$ para algún $d \in \mathbf{N}$. Por lo tanto, $0 + pm = pm = pn = p(d + m) = pd + pm$. Por A_3, $0 = pd$ y $p \neq 0$; entonces $d = 0$ por M_6. Se concluye que $m = n$.

M_5. Supongamos que $m < n$ y $p \neq 0$. Entonces, $n = d + m$ para algún $d \neq 0$. Luego, $pn = pd + pm$ y $pd \neq 0$, por M_6. Por lo tanto, usando A_4, $pm < pn$.

El recíproco se deja como ejercicio. ■

Concluimos con una observación importante acerca de la aritmética de los números naturales. La Teoría Aritmética de los números naturales puede ser enfocada axiomáticamente. Las nociones indefinidas son la constante 0, la operación sucesor y las operaciones binarias + y $\cdot$.

Los Axiomas de Peano son los siguientes:

P1 $0 \in \mathbf{N}$.

P2 Para todo $m, n \in \mathbf{N}$, si $S(m) = S(n)$ entonces $m = n$.

P3 Para todo $n \in \mathbf{N}$, $S(n) \neq 0$.

P4 Para todo $n \in \mathbf{N}$, $n + 0 = n$.

P5 Para todo $m, n \in \mathbf{N}$, $S(m) + n = S(m + n)$.

P6 Para todo $n \in \mathbf{N}$, $n \cdot 0 = 0$.

P7 Para todo $m, n \in \mathbf{N}$, $S(m) \cdot n = (m \cdot n) + n$.

P8 Para todo $n \in \mathbf{N}$, si $n \neq 0$ entonces $n = S(k)$ para algún $k \in \mathbf{N}$.

P9 La Inducción Esquemática. Sea $\mathbf{A}$ una propiedad aritmética (es decir, una propiedad expresable en términos de $+$, $\cdot$, S, 0). Si 0 tiene la propiedad $\mathbf{A}$ y si $\mathbf{A}(k)$ implica $\mathbf{A}(S(k))$ para cada $k \in \mathbf{N}$, entonces todo número natural tiene la propiedad $\mathbf{A}$.

No es difícil verificar que los números naturales y la aritmética aquí definida satisface los Axiomas de Peano, que en realidad originalmente sólo consisten de P1, P2, P3, P8 y P9, los cuales fueron publicados en [P_1]. Peano los tomó como punto de partida para dar un enfoque axiomático a la teoría de los números naturales. Sin embargo, los axiomas se acreditan a Dedekind [D_2].

Ejercicios 5.4

1. Use el Teorema de Recursión para probar la existencia y unicidad de una función (sucesión) con las siguientes propiedades (especifique g).
   (a) $f(m, n) = m^n$ (como es costumbre, uno define $m^0 = 1$, $0^n = 0$ si $n \neq 0$, y deja sin definir 0^0)
   (b) $a_0 = 1$, $a_1 = 2$, $a_2 = 2^2$, $a_3 = 2^{2^2}$, ...
2. Pruebe por inducción que $m + n \geq n$ para todo $m, n \in \mathbf{N}$.
3. Pruebe el recíproco de A_5.
4. Complete la demostración del Teorema 5.21.
5. Pruebe por inducción que para todo $n \in \mathbf{N}$, $n \cdot 0 = 0$ y $n \cdot S(0) = n$.
6. Pruebe el recíproco de M_5.
7. Pruebe que para $a, b \in \mathbf{N}$ con $b \neq 0$, existen elementos únicos q y r de $\mathbf{N}$, tales que $a = qb + r$ donde $r < b$. Este es el *algoritmo de la división* para $\mathbf{N}$.
8. Verifique que las operaciones aritméticas en los números naturales satisfacen los Axiomas de Peano.

6

La Extensión de los Naturales a los Reales

En el capítulo anterior definimos al conjunto de los números naturales $\mathbf{N}$, y en él, dos operaciones binarias $+$ y $\cdot$, y un orden lineal $\leq$. En este capítulo partiremos de $\langle \mathbf{N}, +, \cdot, \leq \rangle$ para construir a los números reales. Para lograrlo construiremos primero a los números enteros y después a los números racionales.

6.1 Diferencias

Definición 6.1 (a) Por una *diferencia* entendemos un par ordenado $(m, n) \in \mathbf{N} \times \mathbf{N}$.

(b) Decimos que una diferencia es *positiva* si $m > n$.

(c) En el conjunto $\mathbf{N} \times \mathbf{N}$ de todas las diferencias, definimos una relación $\underset{d}{\sim}$ por:

$$(m, n) \underset{d}{\sim} (p, q) \text{ si y sólo si } m + q = p + n.$$

Lema 6.2 $\underset{d}{\sim}$ *es una relación de equivalencia en* $\mathbf{N} \times \mathbf{N}$.

Demostración:

Reflexividad. Es claro que para cualquier diferencia (m, n) se cumple que $(m, n) \underset{d}{\sim} (m, n)$.

Simetría. Si $(m, n) \underset{d}{\sim} (p, q)$, entonces $m + q = p + n$, o bien $p + n = m + q$; así, $(p, q) \underset{d}{\sim} (m, n)$.

Transitividad. Si $(m, n) \underset{d}{\sim} (p, q)$ y $(p, q) \underset{d}{\sim} (r, s)$, entonces $m + q = p + n$ y $p + s = r + q$. De esto,

$$\begin{aligned} m + q + s &= p + n + s \\ &= (p + s) + n \\ &= r + q + n. \end{aligned}$$

Y usando la conmutatividad y la cancelación de la adición en $\mathbf{N}$, se tiene que $m+s=r+n$, es decir, $(m,n) \underset{d}{\sim} (r,s)$. ■

Lema 6.3 *(a) Si (m,n) es una diferencia positiva y $(m,n) \underset{d}{\sim} (p,q)$, entonces (p,q) es una diferencia positiva.*

(b) Si (m,n) es positiva, entonces existe una diferencia $(p,0)$ con $p \neq 0$ tal que $(m,n) \underset{d}{\sim} (p,0)$.

Demostración:

(b) Si (m,n) es una diferencia positiva, entonces $m > n$, así que existe $p \in \mathbf{N}\setminus\{0\}$ tal que $m = p+n$. Por lo tanto, $(m,n) \underset{d}{\sim} (p,0)$.

(a) Si (m,n) es una diferencia positiva y si $(m,n) \underset{d}{\sim} (p,q)$, entonces existe $r \in \mathbf{N}\setminus\{0\}$ tal que $(r,0) \underset{d}{\sim} (m,n)$. Por la transitividad de $\underset{d}{\sim}$, se sigue que $(r,0) \underset{d}{\sim} (p,q)$; así que $r+q=p$. Se concluye que $p > q$. Por lo tanto, (p,q) es una diferencia positiva. ■

Definición 6.4 Una operación llamada *adición o suma*, y simbolizada por $+$ es definida para diferencias por

$$(m,n)+(p,q) = (m+p, n+q).$$

Claramente, la adición es una operación binaria en $\mathbf{N}\times\mathbf{N}$. La motivación para la definición es que si $x+n=m$ y $y+q=p$, entonces se sigue que $(x+y)+(n+q)=m+p$.

Lema 6.5 *Si x, y, u y v son diferencias y $x \underset{d}{\sim} u$, $y \underset{d}{\sim} v$, entonces $x+y \underset{d}{\sim} u+v$.*

Demostración:

Supongamos que $(a,b) \underset{d}{\sim} (m,n)$ y que $(c,d) \underset{d}{\sim} (p,q)$. Entonces

$$a+n = m+b \tag{6.1.1}$$

y

$$c+q = p+d. \tag{6.1.2}$$

Sumando las igualdades (6.1.1) y (6.1.2), y usando la conmutatividad y asociatividad de la suma en $\mathbf{N}$ se tiene que

$$(a+c)+(n+q) = (m+p)+(b+d).$$

O sea, $(a+c, b+d) \underset{d}{\sim} (m+p, n+q)$. ■

Lema 6.6 *(a) La adición de diferencias es asociativa y conmutativa.*
(b) La suma de dos diferencias positivas es una diferencia positiva.
(c) La adición es cancelable con respecto a $\underset{d}{\sim}$.

DEMOSTRACIÓN:

Dejamos como ejercicio las partes *(a)* y *(b)*.
(c) Supongamos que $(a,b)+(m,n) \underset{d}{\sim} (a,b)+(p,q)$, entonces

$$(a+m, b+n) \underset{d}{\sim} (a+p, b+q);$$

es decir, $a+m+b+q = a+p+b+n$. Usando la cancelación de la suma en $\mathbf{N}$, se sigue que $m+q = p+n$; así $(m,n) \underset{d}{\sim} (p,q)$. ■

Definición 6.7 Otra operación binaria en $\mathbf{N} \times \mathbf{N}$, que se llama *multiplicación* y es simbolizada por $\cdot$, está definida por

$$(m,n)\cdot(p,q) = (mp+nq, mq+np).$$

Usualmente denotaremos la multiplicación de diferencias x, y por xy en lugar de $x \cdot y$.

Lema 6.8 *Si* x, y, u *y* v *son diferencias tales que* $x \underset{d}{\sim} u$ *y* $y \underset{d}{\sim} v$, *entonces* $xy \underset{d}{\sim} uv$.

Lema 6.9 *(a) La multiplicación de diferencias es asociativa, conmutativa y distribuye sobre la adición.*
(b) El producto de diferencias positivas es una diferencia positiva.
(c) La multiplicación es cancelable con respecto a $\underset{d}{\sim}$ *para diferencias que no sean de la forma* (m,m).

Ejercicios 6.1

1. Pruebe (a) y (b) del Lema 6.6.
2. Pruebe el Lema 6.8.
3. Pruebe el Lema 6.9.

6.2 Los Enteros

Definición 6.10 (a) Definimos un *número entero* como una clase de equivalencia módulo $\underset{d}{\sim}$; y escribimos

$$[x]_i$$

para la clase de equivalencia determinada por la diferencia x.

(b) El conjunto de todos los números enteros es denotado por $\mathbf{Z}$.

(c) Decimos que un número entero es positivo si y sólo si uno de sus miembros es una diferencia positiva.

Se sigue del Lema 6.3 que si $[x]_i$ es positivo, entonces todo miembro de $[x]_i$ es positivo. El conjunto de todos los enteros positivos se denota por $\mathbf{Z}^+$.

Consideremos la siguiente relación de $\mathbf{Z} \times \mathbf{Z}$ en $\mathbf{Z}$:

$$\{(([x]_i, [y]_i), [x+y]_i) : x, y \text{ son diferencias}\}.$$

Acorde al Lema 6.5, esta relación es una función, y en virtud de su forma, es una operación binaria en $\mathbf{Z}$. Llamamos a esta operación *suma* y es simbolizada por $+$. Así,

$$[x]_i + [y]_i = [x+y]_i.$$

La demostración del siguiente resultado se sigue directamente del Lema 6.6.

Proposición 6.11 *La suma de enteros es asociativa, conmutativa y la ley de cancelación es válida. Más aún, la suma de dos enteros positivos es un entero positivo.*

Lema 6.12 *Si x, y son números enteros, entonces existe exactamente un entero z tal que $x + z = y$.*

Demostración:

Sean m, n, p y q números naturales tales que $(m, n) \in x$ y $(p, q) \in y$. Luego basta tomar

$$z = [(p+n, q+m)]_i.$$

La unicidad de z se sigue de la ley de cancelación. ■

Por el resultado anterior se sigue que si x es un entero, entonces existe un único entero, llamado el *inverso aditivo* de x, simbolizado por $-x$ tal que

$$(-x) + x = [(0,0)]_i = x + (-x).$$

Escribiremos $y - x$ para denotar la suma de los enteros y y $-x$; o sea, $y - x = y + (-x)$.

Finalmente, consideremos la relación de $\mathbf{Z} \times \mathbf{Z}$ en $\mathbf{Z}$:

$$\{(([x]_i, [y]_i), [xy]_i) : x, y \text{ son diferencias}\}.$$

Acorde al Lema 6.8 esta relación es una función, que en virtud de su forma, es una operación binaria en $\mathbf{Z}$. Llamamos a esta operación *multiplicación* y es simbolizada por $\cdot$; así,

$$[x]_i \cdot [y]_i = [x \cdot y]_i .$$

Proposición 6.13 *La multiplicación es asociativa y conmutativa, distribuye sobre la adición y tiene la propiedad de la cancelación si* $(0, 0)$ *no es un miembro del factor cancelado. Más aún, el producto de dos enteros positivos es un entero positivo.*

Ahora simplificaremos nuestra notación para los enteros. El primer paso es la observación de que el conjunto de enteros de la forma $[(n, 0)]_i$, con $n \in \mathbf{N}$ y el conjunto de enteros de la forma $[(0, m)]_i$ con $m \in \mathbf{N} \setminus \{0\}$, son ajenos y su unión es $\mathbf{Z}$. En efecto, si $[(p, q)]_i$ es cualquier entero, entonces $p \geq q$ o $p < q$. En el primer caso, $p = q + n$ con $n \in \mathbf{N}$, y por lo tanto,

$$[(p, q)]_i = [(n, 0)]_i .$$

En el segundo caso, $q = p + m$ con $m \in \mathbf{N} \setminus \{0\}$ y

$$[(p, q)]_i = [(0, m)]_i ,$$

lo cual completa la demostración.

La segunda observación es que podemos definir un orden en $\mathbf{Z}$ mediante:

$$[(m, n)]_i <_i [(p, q)]_i$$

si y sólo si $[(p, q)]_i - ([(m, n)]_i) \in \mathbf{Z}^+$. Mostraremos que $<_i$ es un orden lineal estricto para $\mathbf{Z}$; así que $\leq_i$ es un orden total en $\mathbf{Z}$. Más aún, $\leq_i$ es un buen orden en $\{[(0, 0)]_i\} \cup \mathbf{Z}^+$.

La tercera observación es que la función

$$f : \mathbf{N} \to \mathbf{Z}$$

definida por $f(n) = [(n, 0)]_i$, es inyectiva y preserva las operaciones de suma y multiplicación. Más aún, f también preserva el orden, es decir $m \leq n$ implica $f(n) \leq_i f(m)$. Así podemos decir que $\mathbf{Z}$ tiene un subconjunto que es la imagen

orden-isomorfa de $\mathbf{N}$. Esto sugiere llamar a los miembros $[(n,0)]_i$ de $\mathbf{Z}$, los enteros que corresponden a los números naturales y adoptamos 0_i, 1_i, 2_i, etc. como nombres para ellos, es decir, $n_i = [(n,0)]_i$, con $n \in \mathbf{N}$.

Puesto que los restantes enteros son los de la forma $[(0,m)]_i$ con $m \in \mathbf{N} \setminus \{0\}$ y dado que $-[(m,0)]_i = [(0,m)]_i$, a estos los denotaremos como

$$[(0,m)]_i = -m_i,$$

y son llamados *enteros negativos*. Con todas las consideraciones anteriores podemos decir que

$$\mathbf{Z} = \{\cdots, -2_i, -1_i, 0_i, 1_i, 2_i, \cdots\}.$$

Resumimos nuestros resultados concernientes al sistema

$$\langle \mathbf{Z}, +, \cdot, 0_i, 1_i, \mathbf{Z}^+ \rangle$$

de los enteros en el siguiente teorema. Sin embargo, en los ejercicios de esta sección el lector encontrará otras propiedades importantes de este sistema.

Teorema 6.14 *Las operaciones de suma y multiplicación para enteros, junto con 0_i, 1_i y el conjunto $\mathbf{Z}^+$ de enteros positivos tienen las siguientes propiedades. Para cualesquiera enteros x, y, z se cumplen:*

(1) $x + (y + z) = (x + y) + z$.

(2) $x + y = y + x$.

(3) $0_i + x = x$.

(4) Existe un único entero z tal que $x + z = 0_i$; más aún, z es único y es denotado por $-x$.

(5) $x(yz) = (xy)z$.

(6) $xy = yx$.

(7) $1_i \cdot x = x$.

(8) $x(y + z) = xy + xz$.

(9) $xz = yz$, $z \neq 0_i$ *implica* $x = y$.

(10) $0_i \neq 1_i$.

(11) $x, y \in \mathbf{Z}^+$ *implica* $x + y \in \mathbf{Z}^+$.

(12) $x, y \in \mathbf{Z}^+$ *implica* $xy \in \mathbf{Z}^+$.

(13) Exactamente uno de los siguientes enunciados se cumple:

$$x \in \mathbf{Z}^+, \qquad x = 0_i, \qquad -x \in \mathbf{Z}^+.$$

(14) Si $<_i$ es definido por $x <_i$ y si y sólo si $y - x \in \mathbf{Z}^+$, entonces $<_i$ es un orden lineal estricto en $\mathbf{Z}$, y $\leq_i$ un buen orden en $\{0_i\} \cup \mathbf{Z}^+$.

DEMOSTRACIÓN:

El lector debe encargarse de escribir con detenimiento las demostraciones de *(1)* a *(12)*.

(13) Si $x \in \mathbf{Z}$ y $(m, n) \in x$, entonces exactamente ocurre uno de los casos

$$m > n, \qquad m = n, \qquad m < n.$$

por lo que se deduce el resultado.

(14) Por definición de $\mathbf{Z}^+$, claramente $<_i$ es una relación asimétrica. Si $x <_i y$ y $y <_i z$, entonces $y - x \in \mathbf{Z}^+$ y $z - y \in \mathbf{Z}^+$; luego

$$z - x = (z - y) + (y - x) \in \mathbf{Z}^+.$$

Por lo tanto, $x <_i z$. La segunda parte de *(14)* se deduce de que la función

$$\begin{array}{rccc} f: & \mathbf{N} & \longrightarrow & \mathbf{Z}^+ \\ & n & \mapsto & n_i \end{array}$$

es un isomorfismo de orden. ■

Ejercicios 6.2

1. Pruebe la Proposición 6.13.
2. Demuestre las partes (1) a (12) del Teorema 6.14.
3. Demuestre cada una de las siguientes propiedades de los enteros:
   (a) $-(x + y) = -x - y$.
   (b) $(-x)y = -(xy)$.
   (c) $(-x)(-y) = xy$
   (d) $x \in \mathbf{Z}^+$, $y \notin \mathbf{Z}^+$ implica $xy \notin \mathbf{Z}^+$.
   (e) Para cualquier $x \in \mathbf{Z} \setminus \{0_i\}$, se tiene que $x^2 \in \mathbf{Z}^+$.
4. Pruebe cada una de las siguientes propiedades del sistema de los enteros:
   (a) x es positivo si y sólo si $0_i <_i x$
   (b) $x <_i y$ si y sólo si $x + z <_i y + z$.

(c) Si $0 <_i z$, entonces $x <_i y$ si y sólo si $xz <_i yz$.

5. Muestre que cada $x \in \mathbf{Z}$ tiene un sucesor inmediato.

6. Sean $a, b \in \mathbf{Z}$, muestre que el intervalo

$$[a, b] = \{x \in \mathbf{Z} : a \leq_i x \leq_i b\}$$

es finito (de hecho tiene $b - a + 1$ elementos).

7. Sea $(X, \preceq)$ un conjunto linealmente ordenado tal que:
   (a) X no tiene elemento máximo ni mínimo.
   (b) Cualquier subconjunto acotado es finito.
   Entonces $(X, \preceq)$ es isomorfo a $(\mathbf{Z}, \leq_i)$.

8. Sea $A \subseteq \mathbf{Z}$ con $A \neq \emptyset$. Muestre que:

   (a) Si A tiene una cota superior, entonces A tiene un elemento máximo.
   (b) Si A tiene una cota inferior, entonces A tiene un elemento mínimo.

6.3 Los Racionales

Definición 6.15 Un par ordenado $(a, b) \in \mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ se llamará *cociente.* Un cociente se *llamará positivo* si ab es un número entero positivo.

Introducimos una relación en el conjunto de todos los cocientes por

$$(a, b) \underset{q}{\sim} (c, d) \tag{6.3.1}$$

si y sólo si $ad = bc$. Note que esta relación tiene la propiedad

$$(ac, bc) \underset{q}{\sim} (a, b) \text{ si } c \neq 0.$$

Lema 6.16 *La relación en* $\mathbf{Z} \times (\mathbf{Z} \setminus \{0\})$ *descrita por* $\underset{q}{\sim}$*, es una relación de equivalencia.*

Demostración:

Únicamente probaremos la transitividad, puesto que la reflexividad y simetría son claras a partir de las propiedades de $\mathbf{Z}$.

Supongamos que $(a, b) \underset{q}{\sim} (c, d)$ y $(c, d) \underset{q}{\sim} (e, f)$, entonces $ad = bc$ y $cf = de$ con lo que $adf = bcf$, y así $af = be$. ■

Obsérvese que en la demostración anterior se hizo uso de la ley de cancelación en $\mathbf{Z}$, no de algún artificio extraño de división.

Como en el caso de los números enteros, si (a, b) es un cociente positivo, entonces cualquier cociente $\underset{q}{\sim}$-equivalente con (a, b) es positivo. En efecto, si $(a, b) \underset{q}{\sim} (c, d)$, entonces por la transitividad de $\underset{q}{\sim}$ y la observación que precede al Lema 6.16,

$$(ab, b^2) \underset{q}{\sim} (cd, d^2);$$

de aquí que $(ab)d^2 = (cd)b^2$. Como ab y d^2 son enteros positivos, abd^2 es un entero positivo. En virtud del Ejercicio 6.2.(3d), dado que b^2 también es un entero positivo, cd debe ser un entero positivo. Por lo tanto, el cociente (c, d) es un entero positivo.

Ahora es posible dar la definición principal de esta sección.

Definición 6.17 Un *número racional* es una clase de equivalencia módulo $\underset{q}{\sim}$. El número racional determinado por el cociente x será representado por

$$[x]_q .$$

$[x]_q$ se llamará *positivo* si y sólo si contiene un cociente positivo. El conjunto de todos los números racionales positivos es denotado por $\mathbf{Q}^+$.

Lema 6.18 *Sean $[(a, b)]_q$ y $[(c, d)]_q$ números racionales, entonces:*
(a) $[(a, b)]_q + [(c, d)]_q = [(ad + bc, bd]_q$,
(b) $[(a, b)]_q \cdot [(c, d)]_q = [(ac, bd)]_q$,
son operaciones binarias de suma y producto en el conjunto de todos los números racionales, $\mathbf{Q}$.

Demostración:

Si $[(a, b)]_q , [(c, d)]_q \in \mathbf{Q}$, entonces $b \neq 0 \neq d$, con lo cual $bd \neq 0$, que implica $[(ad + bc, bd]_q \in \mathbf{Q}$ y $[(ac, bd)]_q \in \mathbf{Q}$.

Ahora sean $(u, v) \underset{q}{\sim} (a, b)$ y $(x, y) \underset{q}{\sim} (c, d)$. Probaremos que

$$(uy + vx, vy) \underset{q}{\sim} (ad + bc, bd).$$

Como $(u, v) \underset{q}{\sim} (a, b)$, entonces $ub = av$; de la misma manera $xd = cy$, que implica $ubyd = avyd$ y $xdvb = ycvb$; así, $ubyd + xdvb = avyd + ycvb$. De aquí concluimos que $bd(uy + xv) = vy(ad + bc)$, es decir, $(uy + xv, vy)$ es $\underset{q}{\sim}$-equivalente a $(ad + bc, bd)$. Por lo tanto,

$$[(ad + bc, bd)]_q = [(uy + xv, vy)]_q .$$

Análogamente $[(xu, uy)]_q = [(ac, bd)]_q$. Con lo cual las operaciones de suma y producto no dependen de los representantes de las clases. ■

Definamos $a_q = [(a, 1)]_q$ para $a \in \mathbf{Z}$. Claramente

$$\{(a, a_q) : a \in \mathbf{Z}\}$$

es una función de $\mathbf{Z}$ en $\mathbf{Q}$. Más aún, es inyectiva y puesto que

$$\begin{aligned} a_q + b_q &= (a + b)_q, \\ a_q \cdot b_q &= (ab)_q, \end{aligned}$$

las operaciones de suma y producto son preservadas bajo esta función. Finalmente, la imagen a_q de un entero a es un racional positivo si y sólo si a es un entero positivo. Esto último implica que si $<_q$ es definida en términos de los racionales positivos (de manera completamente análoga como se definió $<_i$ en $\mathbf{Z}$), entonces $<_q$ es un orden lineal en $\mathbf{Q}$. Además, para enteros a y b tenemos que $a <_i b$ si y sólo si $a_q <_q b_q$. Así, la función $a \mapsto a_q$ es un isomorfismo de orden. A los elementos a_q de esta imagen orden-isomorfa de $\mathbf{Z}$ en $\mathbf{Q}$ les llamaremos *números racionales enteros*.

En el siguiente teorema se resumen las propiedades del sistema de los números racionales

$$\left\langle \mathbf{Q}, +, \cdot, 0_q, 1_1, \mathbf{Q}^+ \right\rangle.$$

Teorema 6.19 *Las operaciones de suma y multiplicación para los números racionales, junto con* 0_q, 1_q *y el conjunto de los racionales positivos* $\mathbf{Q}^+$, *tienen las siguientes propiedades para racionales cualesquiera* x, y, z*:*

(1) $x + (y + z) = (x + y) + z$.

(2) $x + y = y + x$.

(3) $x + 0_q = x$.

(4) Existe $z \in \mathbf{Q}$ *tal que* $x + z = 0$*; más aún,* z *es único y es denotado por* $-x$.

(5) $x(yz) = (xy)z$.

(6) $xy = yx$.

(7) $1_q \cdot x = x$.

(8) Si $x \neq 0_q$ *entonces existe* $z \in \mathbf{Q}$ *tal que* $xz = 1$*; más aún,* z *es único y es denotado por* x^{-1}.

(9) $x(y + z) = xy + xz$.

(10) $1_q \neq 0_q$.

(11) Si $x, y \in \mathbf{Q}^+$, *entonces* $x + y \in \mathbf{Q}^+$.

(12) Si $x, y \in \mathbf{Q}^+$*, entonces* $xy \in \mathbf{Q}^+$*.*

(13) Exactamente uno de los siguientes enunciados se cumple:

$$x \in \mathbf{Q}^+, \qquad x = 0_q, \qquad -x \in \mathbf{Q}^+.$$

(14) Si P *es la intersección de todos los subconjuntos de* $\mathbf{Q}^+$ *que contienen a* 1_q *y son cerrados bajo la suma, entonces para cada* $x \in \mathbf{Q}^+$*, existen* $a, b \in P$ *tales que* $xb = a$*.*

(15) La relación $<_q$ *dada por*

$$x <_q y \text{ si y sólo si } y - x \in \mathbf{Q}^+,$$

es un orden lineal estricto y tiene las siguientes propiedades:

(i) x *es positivo si y sólo si* $0_q <_q x$*.*

(ii) El cuadrado de un racional diferente de cero es positivo.

(iii) Para cada pareja de racionales x, y *se cumple únicamente una de las siguientes propiedades:*

$$x <_q y, \qquad x = y, \qquad y <_q x.$$

(iv) $x <_q y$ *si y sólo si* $x + z <_q y + z$*, para todo* $z \in \mathbf{Q}$*.*

(v) Si $0_q <_q z$*, entonces* $x <_q y$ *si y sólo si* $xz <_q yz$*.*

Ahora estamos posibilitados para simplificar la notación de los racionales. La siguiente cadena de igualdades muestra que cada racional puede ser escrito en términos de números racionales enteros.

$$\begin{aligned} [(a,b)]_q &= [(a,1_i)]_q \cdot [(1_i,b)]_q \\ &= [(a,1_i)]_q \cdot [(b,1_i)]_q^{-1} \\ &= a_q b_q^{-1}. \end{aligned}$$

En lo posterior dejaremos de usar el subíndice "q" y además convenimos que

$$\frac{a}{b}$$

es otro nombre para el número racional ab^{-1}. De este modo obtenemos la notación familiar para racionales.

En términos prácticos, esto significa que convenimos adoptar nombres de representantes (que son miembros) de números racionales. Para clarificar esta situación, consideremos, por ejemplo, el número racional $[[(2,0)]_i, [(3,0)]_i]_q$. Por nuestra convención, $2/3$ es el nombre de este racional. La proposición

"2/3 = 4/5" significa que 4/5 es otro nombre del mismo racional. Esto es cierto si y sólo si

$$[(2,3)]_q = [(4,5)]_q\,,$$

que de hecho, es verdadero si y sólo si $2 \cdot 5 = 4 \cdot 3$. Puesto que $2 \cdot 5 \neq 4 \cdot 3$, la proposición original es falsa. En general, el mismo tipo de análisis proporciona los siguientes resultados para los racionales:

$$\frac{a}{b} = \frac{c}{d} \text{ si y sólo si } ad = bc,$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$

$$\left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right) = \frac{ac}{bd}.$$

A continuación derivaremos algunas propiedades significativas de los números racionales. En este punto comenzamos a emplear el uso de propiedades elementales de números racionales sin la referencia explícita.

Teorema 6.20 *Entre dos racionales distintos cualesquiera hay otro número racional.*

Demostración:

Sean $x, y \in \mathbf{Q}$ tales que $x <_q y$. Es suficiente probar que

$$x <_q \frac{x+y}{2} <_q y.$$

Para demostrar la primera desigualdad obsérvese que $x + x <_q x + y$. Entonces $2x <_q x + y$. Por lo tanto, $x <_q \frac{x+y}{2}$. Análogamente, $\frac{x+y}{2} <_q y$. ■

Teorema 6.21 (Propiedad Arquimediana) *Si $r, s \in \mathbf{Q}^+$, entonces existe un entero n ($n = n_q$) tal que $s <_q nr$.*

Demostración:

Sean $r = \frac{a}{b}$ y $s = \frac{c}{d}$, donde $a, b, c, d \in \mathbf{N} \setminus \{0\}$. Si n es (el correspondiente entero racional) un entero positivo, entonces $s <_q nr$ si y sólo si $bc <_q nad$. Si seleccionamos $n = 2bc$, como $1 \leq ad$, la desigualdad se satisface. ■

Concluimos la discusión sobre los números racionales introduciendo una función importante.

Definición 6.22 Se define la función *valor absoluto,* $|\cdot| : \mathbf{Q} \to \mathbf{Q}$, como

$$|x| = \begin{cases} x, & si\ x \geq 0 \\ -x, & si\ x < 0 \end{cases}$$

para cada $x \in \mathbf{Q}$.

Teorema 6.23 *Para cualesquiera* $x, y \in \mathbf{Q}$, *tenemos:*

(a) $|x| \geq 0$.
(b) $|xy| = |x|\,|y|$.
(c) $|x + y| \leq |x| + |y|$.
(d) $||x| - |y|| \leq |x - y|$.

Ejercicios 6.3

1. Completar las demostraciones de los Lemas 6.16 y 6.18.

2. Pruebe que la función $a \mapsto a_q$ de $\mathbf{Z}$ en $\mathbf{Q}$ introducida antes del Teorema 6.19 es un isomorfismo de orden.

3. Demuestre el Teorema 6.19 y muestre que el conjunto P que aparece en el inciso (14) de este teorema es simplemente el conjunto de racionales que corresponden a los enteros positivos.

4. Pruebe que la relación $<_q$ para los números racionales puede ser caracterizada como sigue:

$$\frac{a}{b} <_q \frac{c}{d} \quad \text{si y sólo si} \quad abd^2 <_i b^2cd.$$

5. Demuestre cada una de las siguientes propiedades de los números racionales:

   (a) $-(x + y) = -x - y$.
   (b) $(-x)y = -(xy)$.
   (c) $(-x)(-y) = xy$
   (d) $x \in \mathbf{Q}^+$, $y \notin \mathbf{Q}^+$ implica $xy \notin \mathbf{Q}^+$.
   (e) Para cualquier $x \in \mathbf{Q} \setminus \{0_i\}$, se tiene que $x^2 \in \mathbf{Q}^+$.

6. Pruebe el Teorema 6.23.

6.4 Sucesiones de Cauchy de Números Racionales

El conjunto de números racionales $\mathbf{Q}$ contiene subconjuntos no vacíos que son acotados superiormente pero que carecen de supremo. Uno de ellos es

$$S = \left\{x \in \mathbf{Q}^+ : x^2 < 3\right\}.$$

Claramente S es acotado superiormente y no vacío. Sea $u \in \mathbf{Q}$ tal que $u^2 > 3$. Entonces $0 < \frac{3/u+u}{2} < u$, puesto que $\frac{3}{u} < \frac{u^2}{u} = u$; además

$$\left[\frac{u+3/u}{2}\right]^2 = \left[\frac{u-3/u}{2}\right]^2 + 3,$$

por lo que concluimos que S no tiene una mínima cota superior. Esta es una buena razón para tratar de extender $\mathbf{Q}$ a un nuevo conjunto, en el cual no sucedan estas irregularidades y se conserven las propiedades fundamentales de $\mathbf{Q}$.

Definición 6.24 (a) Una *sucesión de números racionales*, que denotamos por $(x_n)_{n=0}^{\infty}$, es una función $x : \mathbf{N} \to \mathbf{Q}$, donde $x(n) = x_n$.

(b) Una sucesión de números racionales $x = (x_n)_{n=0}^{\infty}$, se llama *de Cauchy,* si para todo $\epsilon \in \mathbf{Q}^+$, existe un $n_0 \in \mathbf{N}$ tal que para todo $m, n \geq n_0$,

$$|x_m - x_n| < \epsilon.$$

Intuitivamente las sucesiones de Cauchy de números racionales son aquellas cuyos términos se aproximan unos con otros a partir de un índice suficientemente grande.

Ejemplo 6.25 La sucesión x tal que $x_n = \frac{n+1}{n}$ es una sucesión de Cauchy.

Demostración:

Para probarlo exhibiremos, para cada $\epsilon \in \mathbf{Q}^+$, un $n_0 \in \mathbf{N}$ tal que para todo $m, n \geq n_0$,

$$|x_m - x_n| < \epsilon.$$

Como $|x_m - x_n| = \left|\frac{n-m}{mn}\right| = \left|\frac{1}{m} - \frac{1}{n}\right| < \frac{1}{\min\{m,n\}}$, si tomamos $n_0 \in \mathbf{N}$ tal que $n_0 > \frac{1}{\epsilon} + 1$, entonces para todo $m, n \geq n_0$,

$$|x_m - x_n| < \frac{1}{\min\{m,n\}} < \frac{1}{n_0} < \frac{1}{\frac{1}{\epsilon}} = \epsilon. \quad \blacksquare$$

Ejemplo 6.26 La sucesión x tal que $x_0 = 0$, $x_1 = 1$, y $x_{n+2} = \frac{1}{2}(x_{n+1} + x_n)$ es una sucesión de Cauchy.

DEMOSTRACIÓN:

Por la definición recursiva de x_n es claro que para $m > n$, x_m se encuentra entre x_n y x_{n+1}. Así, si $\epsilon \in \mathbf{Q}^+$ y elegimos $n_0 \in \mathbf{N}$ tal que $2^{n_0} > \frac{1}{\epsilon}$, entonces para todo $m, n \geq n_0$,

$$|x_m - x_n| \leq |x_{n+1} - x_n| \leq \frac{1}{2^n} \leq \frac{1}{2^{n_0}} < \epsilon. \ \blacksquare$$

Dado que los términos de las sucesiones de Cauchy se van aproximando, es de esperar que su rango sea un conjunto acotado. Esto se expresa en el siguiente lema.

Lema 6.27 *Si $(x_n)_{n=0}^{\infty}$ es una sucesión de Cauchy, entonces existe $\delta \in \mathbf{Q}^+$ tal que $|x_n| < \delta$ para todo $n \in \mathbf{N}$.*

DEMOSTRACIÓN:

Correspondiendo al número racional positivo 1 existe por hipótesis $n_0 \in \mathbf{N}$ tal que, para todo $m, n \geq n_0$,

$$|x_m - x_n| < \epsilon.$$

Sea

$$\delta = \max\{|x_0|, |x_1|, \ldots, |x_{n_0}|\} + 1.$$

Claramente, si $n < n_0$, entonces $|x_n| < \delta$. Supongamos que $n \geq n_0$, entonces puesto que $|x_n - x_{n_0}| < 1$ se sigue que

$$|x_n| < |x_{n_0}| + 1 < \delta.$$

Por lo tanto, para todo $n \in \mathbf{N}$, $|x_n| < \delta$. $\blacksquare$

Definición 6.28 Si $x = (x_n)_{n=0}^{\infty}$ y $y = (y_n)_{n=0}^{\infty}$ son sucesiones de números racionales, se definen las sucesiones suma $x + y = (u_n)_{n=0}^{\infty}$ y multiplicación $xy = (v_n)_{n=0}^{\infty}$, por:

$$u_n = x_n + y_n \quad , \quad v_n = x_n y_n,$$

respectivamente.

Claramente, si x, y son sucesiones de números racionales, entonces también lo son $x + y$ y xy. Es un hecho importante que si x y y son sucesiones de Cauchy de números racionales, entonces $x + y$ y xy son sucesiones de Cauchy. En otras palabras, la suma y la multiplicación son operaciones binarias en el conjunto $\mathcal{C}$ de todas las sucesiones de Cauchy de números racionales.

Lema 6.29 *Si x, y son sucesiones de Cauchy, entonces también lo son las sucesiones suma $x + y$, y multiplicación xy.*

DEMOSTRACIÓN:

Probaremos primero lo referente a la suma. Sea $\epsilon \in \mathbf{Q}^+$, por hipótesis existen $n_1, n_2 \in \mathbf{N}$ tales que para todo $m, n \geq n_1$,

$$|x_m - x_n| < \frac{\epsilon}{2}$$

y para todo $m, n \geq n_2$,

$$|y_m - y_n| < \frac{\epsilon}{2}.$$

Entonces para todo $m, n \geq \max\{n_1, n_2\}$,

$$\begin{aligned} |(x_m + y_m) - (x_n + y_n)| &= |(x_m - x_n) + (y_m - y_n)| \\ &\leq |x_m - x_n| + |y_m - y_n| \\ &< \tfrac{\epsilon}{2} + \tfrac{\epsilon}{2} = \epsilon. \end{aligned}$$

Ahora lo referente a la multiplicación. Sea $\epsilon \in \mathbf{Q}^+$; en virtud del Lema 6.27, existen números racionales positivos δ_1 y δ_2 tales que para todo $n \in \mathbf{N}$,

$$|x_n| < \delta_1 \quad \text{y} \quad |y_n| < \delta_2.$$

Además existen $n_1, n_2 \in \mathbf{N}$ tales que para todo $m, n \geq n_1$,

$$|x_m - x_n| < \frac{\epsilon}{2\delta_2}$$

y para todo $m, n \geq n_2$,

$$|y_m - y_n| < \frac{\epsilon}{2\delta_1}.$$

Entonces para todo $m, n \geq \max\{n_1, n_2\}$,

$$\begin{aligned} |x_m y_m - x_n y_n| &= |x_m y_m - x_n y_m + x_n y_m - x_n y_n| \\ &\leq |x_m - x_n|\,|y_m| + |x_n|\,|y_m - y_n| \\ &< \left(\tfrac{\epsilon}{2\delta_2}\right)\delta_2 + \delta_1\left(\tfrac{\epsilon}{2\delta_1}\right) = \epsilon. \quad \blacksquare \end{aligned}$$

Las propiedades básicas de la suma y multiplicación pueden ser resumidas por la afirmación de que ellas satisfacen las propiedades (1) a (8) del Teorema 6.14, donde los elementos distinguidos en (3) y (7) son tomados como la sucesión $\mathbf{0}$ (cuyo valor es 0 para todo n) y la sucesión $\mathbf{1}$ (cuyo valor es 1 para todo n), respectivamente. El negativo de la sucesión de Cauchy x es la sucesión $-x$ tal que $(-x)_n = -x_n$ para todo $n \in \mathbf{N}$.

Introducimos a continuación una relación, la cual será simbolizada por $\underset{c}{\sim}$, en el conjunto $\mathcal{C}$ de todas las sucesiones de Cauchy de números racionales.

Definición 6.30 Sean $x, y \in \mathcal{C}$, definamos una relación $\underset{c}{\sim}$ en $\mathcal{C}$ como $x \underset{c}{\sim} y$ si y sólo si para cada $\epsilon \in \mathbf{Q}^+$, existe $n_0 \in \mathbf{N}$ tal que $|x_n - y_n| < \epsilon$ para todo $n \geq n_0$.

Como una ilustración, considere las sucesiones x y y tales que $x_n = \frac{n+2}{n+1}$ y $y_n = 1$ para todo $n \in \mathbf{N}$. Estas son sucesiones de Cauchy y claramente $x \underset{c}{\sim} y$ puesto que $x_n - y_n = \frac{1}{n+1}$. Es fácil de establecer la siguiente propiedad de esta relación.

Lema 6.31 *La relación $\underset{c}{\sim}$ es una relación de equivalencia en $\mathcal{C}$.*

Definición 6.32 Una sucesión de Cauchy $x \in \mathcal{C}$ se dice *positiva* si existen $\epsilon \in \mathbf{Q}^+$ y $n_0 \in \mathbf{N}$ tales que para todo $n \geq n_0$, $x_n > \epsilon$.

Las propiedades de sustitución esperadas de la relación de equivalencia con respecto a la suma, multiplicación y positividad son formuladas a continuación.

Lema 6.33 *Si $x, y, u, v \in \mathcal{C}$ son tales que $x \underset{c}{\sim} u$ y $y \underset{c}{\sim} v$, entonces $x+y \underset{c}{\sim} u+v$ y $xy \underset{c}{\sim} uv$; además, si x es positiva entonces u es positiva.*

Demostración:

Se mostrará que $xy \underset{c}{\sim} uv$. Sea $\epsilon \in \mathbf{Q}^+$, existen $\delta_1, \delta_2 \in \mathbf{Q}^+$ tales que para todo $n \in \mathbf{N}$, $|y_n| < \delta_1$ y $|u_n| < \delta_2$. Como $x \underset{c}{\sim} u$ entonces existe $n_1 \in \mathbf{N}$ tal que para todo $n \geq n_1$,

$$|x_n - u_n| < \frac{\epsilon}{2\delta_1}$$

y como $y \underset{c}{\sim} v$, existe $n_2 \in \mathbf{N}$ tal que para todo $n \geq n_2$,

$$|y_n - v_n| < \frac{\epsilon}{2\delta_2},$$

entonces para todo $n \geq \max\{n_1, n_2\}$ se tiene que

$$\begin{aligned} |x_n y_n - u_n v_n| &= |x_n y_n - u_n y_n + u_n y_n - u_n v_n| \\ &\leq |x_n - u_n|\,|y_n| + |u_n|\,|y_n v_n| \\ &< \left(\tfrac{\epsilon}{2\delta_1}\right)\delta_1 + \delta_2\left(\tfrac{\epsilon}{2\delta_2}\right) = \epsilon. \end{aligned}$$

Por lo tanto, $xy \underset{c}{\sim} uv$. Análogamente, $x + y \underset{c}{\sim} u + v$.

Por otro lado, si x es positiva existe $\epsilon \in \mathbf{Q}^+$ y $n_1 \in \mathbf{N}$ tal que para todo $n \geq n_1$, $x_n > 2\epsilon$ y existe $n_2 \in \mathbf{N}$ tal que $|x_n - u_n| < \epsilon$ para todo $n \geq n_2$. Entonces para todo $n \geq \max\{n_1, n_2\}$,

$$u_n > x_n - \epsilon > 2\epsilon - \epsilon = \epsilon.$$

Por lo tanto, u es positiva. ■

Con el resultado precedente es fácil probar el siguiente lema, el cual es básico para cuando prestemos atención a la clases de equivalencia de sucesiones de Cauchy módulo $\underset{c}{\sim}$.

Lema 6.34 *La suma y la multiplicación de dos sucesiones de Cauchy positivas son sucesiones de Cauchy positivas. Además, si $x \in \mathcal{C}$, entonces una y sólo una de las siguientes proposiciones es verdadera: x es positiva, $x \underset{c}{\sim} \mathbf{0}$ o $-x$ es positiva.*

Demostración:

Se probará sólo la segunda proposición, dejando como ejercicio la primera.

Claramente se debe cumplir algunas de las proposiciones. Supongamos que no se da $x \underset{c}{\sim} \mathbf{0}$. Entonces existe $\epsilon \in \mathbf{Q}^+$ tal que para todo $n \in \mathbf{N}$ existe $m \in \mathbf{N}$ tal que $|x_n| > 2\epsilon$. También existe $n_0 \in \mathbf{N}$ tal que $|x_m - x_n| < \epsilon$ para todo $m, n \geq n_0$. Entonces existe $p > n_0$ tal que $|x_p| > 2\epsilon$, por lo cual $x_p \neq 0$, por lo que $x_p < 0$ o bien $x_p > 0$. Si $x_p > 0$, entonces $x_p > 2\epsilon$. Luego para todo $n > p$,

$$|x_n - x_p| < \epsilon,$$

lo cual implica que $x_n > x_p - \epsilon > 2\epsilon - \epsilon = \epsilon$. Por lo tanto, x es positiva.

Si $x_p < 0$, aplicando un razonamiento análogo a $-x$, tenemos que $-x$ es positiva. ■

Lema 6.35 *Si $x \in \mathcal{C}$ no es equivalente a $\mathbf{0}$ módulo $\underset{c}{\sim}$, entonces existe $y \in \mathcal{C}$ tal que $xy \underset{c}{\sim} \mathbf{1}$.*

Demostración:

Por el lema anterior, si es falso que $x \underset{c}{\sim} \mathbf{0}$, entonces existen $\epsilon \in \mathbf{Q}^+$ y $n_0 \in \mathbf{N}$, tales que $|x_n| \geq \epsilon$ para todo $n \geq n_0$. Considérese la siguiente sucesión: $x'_n = \epsilon$ si $n < n_0$ y $x'_n = x_n$ si $n \geq n_0$. Entonces $(x'_n)_{n=0}^{\infty} \in \mathcal{C}$ y $x \underset{c}{\sim} (x'_n)_{n=0}^{\infty}$; más aún, para todo $n \in \mathbf{N}$, $|x'_n| \geq \epsilon$.

Como $x'_n \neq 0$ para todo $n \in \mathbf{N}$, sea y la sucesión $(y_n)_{n=0}^{\infty}$ en donde

$$y_n = \frac{1}{x'_n}.$$

Afirmamos que $y \in \mathcal{C}$. En efecto, sea $\eta \in \mathbf{Q}^+$. Como $(x'_n)_{n=0}^{\infty} \in \mathcal{C}$, existe $n_1 \in \mathbf{N}$ tal que $|x'_m - x'_n| < \eta\epsilon^2$ para todo $m, n \geq n_1$. Además,

$$\frac{1}{x'_m x'_n} \leq \frac{1}{\epsilon^2}$$

puesto que $|x'_n| \geq \epsilon$. Entonces, para todo $m, n \geq n_1$,

$$|y_m - y_n| < \eta,$$

lo que implica que $y \in \mathcal{C}$.

Es claro que $x'y \underset{c}{\sim} \mathbf{1}$. ■

Ejercicios 6.4

1. Pruebe que la sucesión x tal que

$$x_n = 1 - \frac{1}{3} + \frac{1}{5} - \cdots + \frac{(-1)^n}{2n+1}$$

es una sucesión de Cauchy.

2. Pruebe que la sucesión x tal que

$$x_n = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!}$$

es una sucesión de Cauchy.

3. Demuestre que la suma y multiplicación de sucesiones de Cauchy satisfacen (1) a (8) del Teorema 6.14.

4. Pruebe el Lema 6.31.

5. Complete la demostración del Lema 6.33.

6. Complete la demostración del Lema 6.34.

6.5 Los Reales

Definición 6.36 Definimos un *número real* como una clase de equivalencia módulo $\underset{c}{\sim}$ de sucesiones de Cauchy de números racionales.

El número real determinado por la sucesión de Cauchy x lo denotamos como

$$[x]_r .$$

El conjunto de los números reales es $\mathbf{R} = \mathcal{C}/\underset{c}{\sim}$. Un número real es llamado *positivo* si y sólo si contiene una sucesión de Cauchy positiva. En vista del Lema 6.33, si $[x]_r$ es positivo, entonces cada uno de sus miembros es positivo. El conjunto de todos los números reales positivos es simbolizado por $\mathbf{R}^+$.

De modo natural se definen las operaciones de suma y multiplicación de números reales como:

$$[x]_r + [y]_r = [x+y]_r$$
$$[x]_r \cdot [y]_r = [xy]_r ,$$

que, en virtud de los lemas de la sección anterior, son operaciones binarias en el conjunto de los números reales. También definimos un orden en $\mathbf{R}$ por:

$$x <_r y \text{ si y sólo si } y - x \in \mathbf{R}^+.$$

Es de esperar que este orden herede todas las propiedades de $<_q$. En efecto, el orden $\leq_r$ que resulta a partir de $<_r$ es un orden total en $\mathbf{R}$. Además, $\mathbf{R}$ tiene un sistema orden-isomorfo a $\mathbf{Q}$; pues si $a \in \mathbf{Q}$, entonces $(a)_{n=0}^{\infty} \in \mathcal{C}$ y en consecuencia existe un único número real $[a]_r$ que contiene a $(a)_{n=0}^{\infty}$; así la función $a \mapsto [a]_r$ es una inyección y un isomorfismo sobre su imagen. Más aún, es fácil probar que esta función también preserva las operaciones de suma y multiplicación.

Los números reales correspondientes a los números racionales 0_q y 1_q son simbolizados por 0_r y 1_r.

Teorema 6.37 *El sistema* $\langle \mathbf{R}, +, \cdot, 0_r, 1_r, \mathbf{R}^+ \rangle$ *tiene las propiedades (1) a (13) y (15) del Teorema 6.19.*

La definición de la función valor absoluto se extiende a los números reales de manera obvia y las relaciones enunciadas en el Teorema 6.23 siguen siendo válidas cuando consideramos el valor absoluto de números reales.

Los resultados hasta ahora obtenidos muestran que $\mathbf{R}$ es una extensión de $\mathbf{Q}$, donde las propiedades fundamentales de los números racionales son conservadas (un ejemplo importante es que la función $a \mapsto [a]_r$ preserva el orden). Probaremos ahora que todo conjunto no vacío y acotado superiormente,

admite una mínima cota superior, pero ello requiere de algunos resultados preliminares.

En lo posterior haremos referencia a números naturales, enteros y racionales de $\mathbf{R}$, pues *abusando* de notación podemos decir que $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subseteq \mathbf{R}$ (dado que $\mathbf{R}$ tiene una "copia" de cada uno de estos sistemas); por lo cual, omitiremos de ahora en adelante el subíndice r.

En el siguiente teorema se presenta una de las propiedades más importantes que enlazan a $\mathbf{Q}$ y $\mathbf{R}$, se conoce como la propiedad de *densidad* de $\mathbf{Q}$ en $\mathbf{R}$.

Teorema 6.38 *Entre dos reales distintos cualesquiera hay un número racional.*

DEMOSTRACIÓN:

Sean $x, y \in \mathbf{R}$ tales que $x < y$, y sean $a \in x$ y $b \in y$. Existen $\epsilon \in \mathbf{Q}^+$ y $n_1 \in \mathbf{N}$ tales que para todo $n \geq n_1$, $b_n - a_n > 4\epsilon$. Además como $a, b \in \mathcal{C}$, entonces existen $n_2, n_3 \in \mathbf{N}$ tales que para todo $m, n \geq n_2$,

$$|a_m - a_n| < \epsilon,$$

y para todo $m, n \geq n_3$,

$$|b_m - b_n| < \epsilon.$$

Sean $n_0 = \max\{n_1, n_2, n_3\} + 1$ y $s \in \mathbf{Q}$ tal que $\epsilon < s < 2\epsilon$, que existe en virtud del Teorema 6.20. Ahora consideremos el número real z correspondiente al número racional $a_{n_0} + s$. Entonces $a_n - a_{n_0} < \epsilon$ para todo $n \geq n_0$.

Puesto que $a_{n_0} - a_n > -\epsilon$ para todo $n \geq n_0$,

$$a_{n_0} + s - a_n > s - \epsilon > 0,$$

esto significa que la sucesión de Cauchy

$$(a_{n_0} + s, a_{n_0} + s, \ldots, a_{n_0} + s, \ldots) - a$$

es positiva y dado que esta sucesión es un miembro de $z - x$, esto significa que $x < z$.

Usando la identidad

$$b_n - (a_{n_0} + s) = (b_{n_0} - a_{n_0}) + (b_n - b_{n_0}) + s$$

se sigue, con un argumento similar, que $y - z \in \mathbf{R}^+$; lo que implica $z < y$. Por lo tanto, $x < z < y$. ■

Lema 6.39 *Si $x, y \in \mathcal{C}$ y si existe $n_0 \in \mathbf{N}$ tal que para todo $n \geq n_0$, $x_n \leq y_n$, entonces $[x]_r \leq [y]_r$.*

Si $x, y \in \mathcal{C}$ y existe $n_0 \in \mathbf{N}$ tal que para todo $n \geq n_0$, $x_n < y_n$, entonces $[x]_r \leq [y]_r$, es decir, no se puede garantizar la desigualdad estricta.

El siguiente teorema es una generalización del Teorema 6.21 para el sistema de los números reales.

Teorema 6.40 (Propiedad Arquimediana) *Si $x, y \in \mathbf{R}^+$, entonces existe $n \in \mathbf{N}$ tal que $nx > y$.*

Demostración:

Sea $b \in y$, entonces existe $\delta \in \mathbf{Q}^+$ tal que $|b_n| < \delta$ para todo $n \in \mathbf{N}$. Si d es el número real correspondiente a $(\delta)_{n=0}^{\infty}$, entonces $y \leq d$. También, el supuesto $0 < x$ implica la existencia de $s \in \mathbf{Q}$ tal que $0 < s < x$. Sea $t \in \mathbf{Q}$ tal que $y \leq t \leq d$. Por la Propiedad Arquimediana para racionales, existe $n \in \mathbf{N}$ tal que $ns > t$. Entonces $nx > ns > t > y$. ■

Teorema 6.41 *Todo subconjunto no vacío de números reales que tiene una cota superior, tiene una mínima cota superior.*

Demostración:

Sea A un conjunto que satisface la hipótesis del teorema. Por el Teorema 6.40 existen m y M tales que m no es cota superior de A y M sí es cota superior de A. Entonces podemos inferir la existencia de un entero b_0 tal que b_0 es cota superior de A pero $b_0 - 1$ no lo es.

Definamos la sucesión $(b_n)_{n=0}^{\infty}$ inductivamente como sigue:

$$b_n = \begin{cases} b_{n-1} - \frac{1}{2^n}, & \text{si } b_{n-1} - \frac{1}{2^n} \text{ es cota superior de } A \\ \\ b_{n-1}, & \text{si } b_{n-1} - \frac{1}{2^n} \text{ no es cota superior de } A. \end{cases}$$

Entonces para todo $n \in \mathbf{N}$, b_n es cota superior de A, y podemos probar por un argumento de inducción que

$$b_n - \frac{1}{2^n}$$

no lo es. De este modo, para $m > n$,

$$b_n - \frac{1}{2^n} < b_m, \tag{6.5.1}$$

además es claro que para todo $m \geq n$,

$$b_m \leq b_n. \tag{6.5.2}$$

Combinando las desigualdades (6.5.1) y (6.5.2) tenemos que $|b_m - b_n| < \frac{1}{2^n}$. Se sigue de aquí que si $n_0 \in \mathbf{N}$ y $m, n \geq n_0$, entonces

$$|b_m - b_n| < \frac{1}{2^{n_0}};$$

o sea, $b = (b_n)_{n=0}^{\infty}$ es una sucesión de Cauchy.

Sea u el número real que determina b. Entonces por el Lema 6.39, por la desigualdad (6.5.1) y usando la desigualdad (6.5.2) para todo n tenemos que:

$$b_n - \frac{1}{2^n} \leq u, \tag{6.5.3}$$

$$u \leq b_n. \tag{6.5.4}$$

Demostraremos que u es una cota superior de A. Supongamos lo contrario, es decir, supongamos que existe un $a \in A$ tal que $u < a$. Entonces, existe un $n \in \mathbf{N}$ tal que $2^n > \frac{1}{a-u}$; luego, $\frac{1}{2^n} < a-u$. Si esto lo sumamos a la desigualdad (6.5.3) tenemos

$$b_n - \frac{1}{2^n} + \frac{1}{2^n} < u + a - u,$$

lo cual implica que $b_n < a$, que es una contradicción. Por lo tanto, u es una cota superior de A.

Finalmente probaremos que u es la mínima de las cotas superiores de A. Supongamos que v es cota superior de A y que $v < u$, entonces existe un $n \in \mathbf{N}$ tal que $\frac{1}{2^n} < u - v$. Como $b_n - \frac{1}{2^n}$ no es cota superior de A, entonces existe $a \in A$ tal que $b_n - \frac{1}{2^n} < a$; así

$$b_n - \frac{1}{2^n} < v,$$

por lo que

$$\frac{1}{2^n} + b_n - \frac{1}{2^n} < u - v + v;$$

o sea, $b_n < u$, que contradice la desigualdad (6.5.4). Por lo tanto, u es la mínima cota superior de A. ■

Este último teorema es quien proporciona la característica primordial que hace diferente al sistema de los números reales. Puede demostrarse que

$$\left\langle \mathbf{R}, +, \cdot, 0_r, 1_r, \mathbf{R}^+ \right\rangle$$

es el "único" sistema con esta propiedad; es decir, en caso de existir otro sistema que satisface todas las propiedades en los enunciados de los teoremas 6.37 y 6.41, entonces también existe un isomorfismo de orden entre ellos que además preserva las operaciones de suma y multiplicación. Una demostración completa de esta afirmación se puede consultar en el capítulo 29 del libro de Spivak [S_9]. De hecho, existen otras maneras de presentar el sistema de los números reales, por ejemplo, el de cortaduras de Dedekind, que se encuentra en el clásico libro de Landau [L_1]. También suele introducirse por una lista de trece axiomas, pero podemos decir que: *no importa el método de presentación de* $\mathbf{R}$, *siempre obtenemos, en esencia, el mismo objeto.*

Ahora como una consecuencia del teorema anterior mostraremos, después de dos lemas, que toda sucesión de Cauchy de números reales tiene límite. Una sucesión x de números reales es una sucesión tal que $x_n \in \mathbf{R}$ para cada $n \in \mathbf{N}$. Una *sucesión de Cauchy de números reales* es una sucesión de números reales tal que para cualquier número real positivo ϵ existe $n_0 \in \mathbf{N}$ tal que

$$|x_m - x_n| < \epsilon$$

para todo $m, n \geq n_0$.

Ahora definiremos la noción de límite. Esta noción es la habitual del Cálculo Diferencial e Integral y, de hecho, del Análisis en general.

Definición 6.42 El número real y *es límite de la sucesión* x de números reales si y sólo si para todo número real positivo ϵ existe un $n_0 \in \mathbf{N}$ tal que

$$|x_n - y| < \epsilon$$

para todo $n \geq n_0$.

Ejemplo 6.43 Toda sucesión constante de números reales tiene límite.

La prueba del siguiente lema es un ejercicio.

Lema 6.44 *El límite de una sucesión de números reales es único.*

Así, si la sucesión x de números reales tiene a y como un límite, entonces y es el único limite y se justifica la siguiente notación familiar para y:

$$\lim_{n\to\infty} x_n = y.$$

Una sucesión de números reales $(x_n)_{n=0}^{\infty}$ se llama creciente si $x_n \leq x_{n+1}$ para cada $n \in \mathbf{N}$, y decreciente si $x_{n+1} \leq x_n$ para cada $n \in \mathbf{N}$. Con esta terminología podemos dar el siguiente ejemplo que nos proporciona una amplia variedad de sucesiones con límite.

Ejemplo 6.45 Toda sucesión de números reales decreciente (creciente) que está acotada inferiormente, es decir, tal que existe $M \in \mathbf{R}$ con $M \leq x_n$, para todo $n \in \mathbf{N}$ (respectivamente, superiormente: $x_n \leq M$, para todo $n \in \mathbf{N}$), tiene límite.

DEMOSTRACIÓN:

Haremos la prueba para sucesiones decrecientes. Sean

$$y = \inf \{x_n : n \in \mathbf{N}\}$$

y $\epsilon > 0$, entonces $y + \epsilon$ no puede ser cota inferior del conjunto $\{x_n : n \in \mathbf{N}\}$. Así, existe $n_0 \in \mathbf{N}$ tal que

$$y \leq x_{n_0} < y + \epsilon.$$

Como la sucesión $(x_n)_{n=0}^{\infty}$ es decreciente, para todo $n \geq n_0$ tenemos que $y \leq x_n \leq x_{n_0} < y + \epsilon$. Por lo tanto, para todo $n \geq n_0$,

$$|y - x_n| < \epsilon. \blacksquare$$

Lema 6.46 *Sea $(a_n)_{n=0}^{\infty}$ una sucesión de números racionales y sea x la sucesión de números reales tal que para cada $n \in \mathbf{N}$, $x_n = [(a_n)_{m=0}^{\infty}]_r$ es el número real correspondiente a a_n. Entonces x es una sucesión de Cauchy de números reales si y sólo si a es una sucesión de Cauchy de números racionales. Además, si $(a_n)_{n=0}^{\infty}$ es una sucesión de Cauchy de números racionales y z es el número real que ella define, entonces* $\lim_{n\to\infty} a_n = z$.

DEMOSTRACIÓN:

Demostraremos solamente la segunda afirmación. Sea ϵ un número real positivo y sea $\delta = [(d)_{n=0}^{\infty}]_r$ un número racional tal que $0 < \delta < \epsilon$. Como $(a_n)_{n=0}^{\infty}$ es por hipótesis una sucesión de Cauchy, existe $n_0 \in \mathbf{N}$ tal que

$$|a_n - a_m| < d,$$

para $m, n \geq n_0$. Como $a_n - a_m < d$, si $m, n \geq n_0$, se sigue que

$$[(a_n)_{m=0}^{\infty} - (a_m)_{m=0}^{\infty}]_r \leq \delta$$

para cada $n \geq n_0$ (por el Lema 6.39), o en otras palabras,

$$x_n - z \leq \delta$$

siempre que $n \geq n_0$. Similarmente, la desigualdad $a_m - a_n < d$ implica que

$$z - x_n \leq \delta$$

cuando $n \geq n_0$. Por lo tanto, para todo $n \geq n_0$,

$$|x_n - z| \leq \delta < \epsilon. \ \blacksquare$$

Teorema 6.47 *Una sucesión de números reales tiene límite si y sólo si es una sucesión de Cauchy de números reales.*

Demostración:

Se deja como un ejercicio probar que si una sucesión de números reales tiene límite, entonces es de Cauchy.

Demostraremos la suficiencia. Supongamos que u es una sucesión de Cauchy de números reales. Para cada $n \in \mathbf{N}$, $u_n < u_n + \frac{1}{n}$ y por lo tanto (Teorema 6.38), existe un número racional $x_n \in \mathbf{R}$ tal que

$$u_n < x_n < u_n + \frac{1}{n}.$$

Sea ϵ un número real positivo, entonces existe $n_1 \in \mathbf{N}$ tal que $n_1 > \frac{3}{\epsilon}$ y, por tanto, para todo $n \geq n_1$,

$$|u_n - x_n| < \frac{\epsilon}{3} \tag{6.5.5}$$

Más aún, x es una sucesión de Cauchy de números racionales, ya que

$$|x_m - x_n| \leq |x_m - u_m| + |u_m - u_n| + |u_n - x_n|,$$

y para m y n suficientemente grandes cada sumando del lado derecho es menor que $\frac{\epsilon}{3}$. Sea a_n el número racional en $\mathbf{Q}$ al cual corresponde x_n. Por el Lema 6.46, $a = (a_n)_{n=0}^{\infty}$ es una sucesión de Cauchy de números racionales y por lo tanto, define un número real y. Además, por el Lema 6.46

$$\lim_{n \to \infty} x_n = y.$$

De lo anterior se deduce la existencia de algún $n_2 \in \mathbf{N}$ tal que

$$|x_n - y| < \frac{\epsilon}{2}, \tag{6.5.6}$$

para todo $n \geq n_2$. Se infiere de las desigualdades (6.5.5) y (6.5.6) que para todo $n \geq \max\{n_1, n_2\}$,

$$|u_n - y| \leq |u_n - x_n| + |x_n - y| < \frac{\epsilon}{3} + \frac{\epsilon}{2} < \epsilon,$$

lo cual significa que

$$y = \lim_{n\to\infty} u_n. \ \blacksquare$$

Finalmente estableceremos la posibilidad de representar a un número real por una expresión decimal. Para cada número real no negativo x, denotaremos por $\lfloor x \rfloor$ al mayor entero menor o igual a x; es decir,

$$\lfloor x \rfloor = \max \{n \in \mathbf{N} : n \leq x\}.$$

Teorema 6.48 *Sea r un número entero mayor o igual a 2. A cada número real no negativo, x corresponde una sucesión $(d_n)_{n=0}^{\infty}$ de enteros, los cuales están unívocamente determinados por x (relativo a r), tales que:*

(a) $d_0 = \lfloor x \rfloor$,

(b) $0 \leq d_n < r$ para cada $n \geq 1$,

(c) la sucesión cuyos términos están definidos recursivamente por

$$y_0 = d_0$$
$$y_{n+1} = y_n + \frac{d_{n+1}}{r^{n+1}}$$

es una sucesión de Cauchy y $\lim_{n\to\infty} y_n = x$.

Demostración:

Sean r un entero mayor o igual a 2, x un número real no negativo y $d_0 = \lfloor x \rfloor$. Entonces

$$xr = d_0 r + x_1$$

para algún número x_1 tal que $0 \leq x_1 < r$. Si $d_1 = \lfloor x_1 \rfloor$, se tiene que

$$x_1 r = d_1 r + x_2,$$

para algún $0 \leq x_2 < r$. En general, definamos x_n por

$$x_{n-1} r = d_{n-1} r + x_n$$

y sea $d_n = \lfloor x_n \rfloor$. Entonces

$$x = d_0 + \frac{d_1}{r} + \frac{d_2}{r^2} + \cdots + \frac{d_n}{r^n} + \frac{x_{n+1}}{r^{n+1}},$$

donde $0 \leq x_{n+1} < r$. Por lo tanto,

$$0 \leq x - \left(d_0 + \frac{d_1}{r} + \frac{d_2}{r^2} + \cdots + \frac{d_n}{r^n} \right) < \frac{1}{r^n}.$$

De acuerdo a la definición de y_n en *(c)*, esto lo podemos escribir como

$$0 \leq x - y_n < \frac{1}{r^n},$$

por lo que se sigue que $|x - y_n| < \frac{1}{r^n}$, y así

$$\lim_{n\to\infty} y_n = x.$$

La prueba de la unicidad (relativa a r) de la sucesión correspondiente a x se deja como un ejercicio. ■

Si $r = 10$ en el teorema precedente obtenemos la familiar representación decimal de un número real no negativo; cuando $r = 2$ se obtiene la representación diádica, etc. Por ejemplo para la representación decimal del conocido número π tenemos que: $d_0 = 3,\ d_1 = 1,\ d_2 = 4,\ d_3 = 1,\ d_4 = 5,\ d_5 = 9,\ d_6 = 2,\ d_7 = 6,\ d_8 = 5\,,\ d_9 = 3,\ d_{10} = 5,\ d_{11} = 8,\ d_{12} = 9,\ d_{13} = 7,\ d_{14} = 9,\ d_{15} = 3,\ d_{16} = 2,\ d_{17} = 3,\ d_{18} = 8,\ d_{19} = 4,\ d_{20} = 6$, etc. Por lo cual habitualmente lo escribimos como:

$$\pi = 3.14159265358979323846\ldots\ .$$

Ejercicios 6.5

1. Pruebe que la función $a \mapsto [a]_r$ es un isomorfismo de orden entre $\mathbf{Q}$ y un subconjunto de $\mathbf{R}$. Además, pruebe que esta función preserva las operaciones de suma y multiplicación.

2. Demuestre el Teorema 6.37.

3. Pruebe el Lema 6.39.

4. Dar un ejemplo de dos sucesiones x y y tales que $x_n < y_n$ para cada $n \in \mathbf{N}$, pero que $[x]_r = [y]_r$.

5. Pruebe la afirmación realizada en la prueba del Teorema 6.41 de que $b_n - \frac{1}{2^n}$ no es una cota superior de A.

6. Sean A y B subconjuntos no vacíos de números reales. Demuestre que si A y B están acotados superiormente, entonces

   $$C = \{x + y : x \in A,\ y \in B\}$$

   está acotado superiormente y $\sup C = \sup A + \sup B$.

7. Sean A y B subconjuntos no vacíos de números reales positivos. Demuestre que si A y B están acotados superiormente, entonces

$$C = \{x \cdot y : x \in A,\ y \in B\}$$

está acotado superiormente y $\sup C = \sup A \cdot \sup B$.

8. Sea $\{A_\alpha\}_{\alpha \in I}$ una familia de subconjuntos de $\mathbf{R}$ no vacíos y acotados superiormente, y sea $B = \{\sup A_\alpha : \alpha \in I\}$. Demuestre que $A = \bigcup_{\alpha \in I} A_\alpha$ está acotado superiormente si y sólo si B está acotado superiormente. ¿Qué relación existe entre $\sup A$ (si existe) y $\sup B$?

9. Una función $f : A \subseteq \mathbf{R} \to \mathbf{R}$ se llama continua en $a \in A$ si para cada $\epsilon > 0$ existe $\delta > 0$ tal que para $|h| < \delta$ y $a+h \in A$, $|f(a+h) - f(a)| < \epsilon$. Demuestre que si f es una función continua en cada punto de un intervalo $[a, b]$ tal que $f(a) < 0$ y $f(b) > 0$, entonces existe un número c tal que $a < c < b$ y $f(c) = 0$. (Sugerencia: defina c como el supremo de $\{x \in [a, b] : f(x) < 0\}$.)

10. Suponga que las funciones polinomiales son continuas en $\mathbf{R}$. Sea f la función polinomial tal que $f(x) = x^n - a$, donde $n \in \mathbf{N}$ y $a \in \mathbf{R}^+$. Pruebe que existe exactamente un número real positivo c tal que $f(c) = 0$. Este número c se llama n-ésima raíz de a y se denota por $\sqrt[n]{a}$ o $a^{\frac{1}{n}}$.

11. Pruebe usando el ejercicio anterior que hay números reales que no son racionales.

12. Si $a > 0$, $b > 0$, y $n \in \mathbf{N}$, pruebe que

$$\sqrt[n]{a}\,\sqrt[n]{b} = \sqrt[n]{ab}.$$

13. Pruebe el Lema 6.44.

14. Pruebe la primera afirmación del Lema 6.46.

15. Pruebe la necesidad del Teorema 6.47.

16. Pruebe la unicidad de la sucesión $(d_n)_{n=0}^{\infty}$ asegurada en el Teorema 6.48.

7

Cardinalidad

7.1 Introducción

Una de las distinciones fundamentales en matemáticas es la existente entre conjunto finito e infinito. La diferencia es tan comprensible intuitivamente que, incluso en la ausencia de una definición formal, no hay duda alguna de si un conjunto dado es finito o infinito. Anteriormente sugerimos que los conjuntos finitos pueden ser definidos como aquellos conjuntos que son el rango de alguna sucesión finita; o sea, aquellos que pueden expresarse en la forma $\{a_1, a_2, \ldots, a_n\}$. En la segunda sección de este capítulo daremos un significado preciso de esta proposición. La idea es más o menos así: al contar la colección S de sillas de un salón lo que cotidianamente hacemos es establecer una biyección entre la colección de sillas y un número natural $n = \{0, 1, 2, \ldots, n-1\}$. En tal caso decimos que el número de elementos o cardinalidad de S es n.

¿Cómo "contaríamos" los elementos que forman el conjunto de los números pares o el conjunto de números reales x tales que $0 \leq x \leq 1$? Esta pregunta nos lleva a cuestionarnos: ¿Qué podremos entender por la cardinalidad de conjuntos infinitos? Otro problema es: ¿Tendrá sentido hablar de número cardinal como el número de elementos de un conjunto? Para los conjuntos finitos la respuesta es indudablemente sí; por ejemplo, podemos decir que el número cardinal de la colección de sillas S es n. Imitando lo dicho para conjuntos finitos, haremos una extensión del concepto de número, es decir, hablando vagamente, podemos decir que el número cardinal de un conjunto es la propiedad común que tienen el conjunto y todos los conjuntos equivalentes a él; o sea, aquellos que contienen la misma cantidad de elementos. Ya sabemos que no tenemos facultad de decir que el número cardinal de un conjunto arbitrario X es igual al conjunto de todos los conjuntos equivalentes a X, pues no hay un conjunto así de grande. Lo que sigue es, sugerido por analogía con los números naturales, definir el número cardinal de un conjunto X como un conjunto equivalente a X elegido en forma particularmente cuidadosa.

7.2 Conjuntos Finitos

Definición 7.1 (a) Un conjunto S es *finito* si existe una función biyectiva f de S en algún número natural n. Si éste es el caso, entonces decimos que S tiene n elementos o que el número cardinal de S es n y denotamos $|S| = \#(S) = n$.

(b) Un conjunto S es *infinito* si no es finito.

Las primeras observaciones que debemos hacer es que, en efecto, $\#(n) = n$. Por otra parte, es conveniente verificar inmediatamente que no hay un conjunto S tal que $\#(S) = n$, $\#(S) = m$ simultáneamente, y $n \neq m$. Esto se sigue del siguiente lema.

Lema 7.2 *Si $n \in \mathbf{N}$, entonces no existe una función inyectiva de n sobre un subconjunto propio $X \subset n$.*

Demostración:

Por inducción sobre n. Para $n = 0$, la afirmación es trivialmente cierta. Supongamos que es cierto para n, probaremos que también lo es para $n+1$. Si la afirmación es falsa para $n+1$, entonces existe una función inyectiva f de $n+1$ en algún $X \subset n+1$. Hay dos posibles casos: $n \in X$ o $n \notin X$. Si $n \notin X$, entonces $X \subseteq n$, y $f\,|_n$ manda n sobre el subconjunto propio $X \setminus \{f(n)\}$ de n, lo cual es imposible. Si $n \in X$, entonces $n = f(k)$ para algún $k \leq n$. Consideremos la función g en n definida como sigue:

$$g(i) = \begin{cases} f(i), & \text{para todo } i \neq k,\ i < n \\ f(n) & \text{si } i = k < n. \end{cases}$$

La función g es inyectiva y manda n sobre $X \setminus \{n\}$, un subconjunto propio de n; una contradicción. ■

Corolario 7.3 *(a) Si $m \neq n$, entonces no existe una biyección de m en n.*

(b) Si $\#(S) = m$ y $\#(S) = n$ entonces $m = n$.

(c) $\mathbf{N}$ es infinito.

Demostración:

Para ver que *(c)* se cumple, asumamos que hay una biyección f de $\mathbf{N}$ en algún $n \in \mathbf{N}$. Entonces $f\,|_n$ manda n sobre un subconjunto propio de n, lo cual es una contradicción. ■

Teorema 7.4 *Si X es un conjunto finito y $Y \subseteq X$, entonces Y es finito. Más aún, $\#(Y) \leq \#(X)$.*

DEMOSTRACIÓN:

Podemos suponer que $Y \neq \emptyset$. Como X es finito,

$$X = \{x_0, x_1, \ldots, x_{n-1}\},$$

donde $(x_i)_{i=0}^{n-1}$ es una sucesión inyectiva. Para mostrar que Y es finito, construiremos una sucesión finita inyectiva cuyo rango es Y. Usaremos el Teorema de Recursión en la versión del Ejercicio 5.3.4. Sea

$$k_0 = \min\{k : x_k \in Y\},$$

y si $\{k : k > k_i,\ k < n \text{ y } x_k \in Y\} \neq \emptyset$, sea

$$k_{i+1} = \min\{k : k > k_i,\ k < n,\ \text{y } x_k \in Y\ \}.$$

Esto define una sucesión finita $(k_i)_{i=0}^{m-1}$. Al hacer $y_i = x_{k_i}$ para todo $i < m$, entonces $Y = \{y_i : i < m\}$. Se deja de ejercicio mostrar que $m \leq n$. ■

Teorema 7.5 *Si X es un conjunto finito y f es una función, entonces $f(X)$ es finito. Más aún, $\#(f(X)) \leq \#(X)$.*

DEMOSTRACIÓN:

Sea $X = \{x_0, x_1, \ldots, x_{n-1}\}$. Nuevamente usaremos recursión para construir una sucesión finita e inyectiva cuyo rango es $f(X)$. Ahora usaremos la versión $f(n+1) = g(f\ |_n)$. La construcción es como sigue (los detalles se dejan al lector):

$k_0 = 0$, k_{i+1} es el mínimo $k > k_i$ tal que $k < n$ y $f(x_k) \neq f(x_{k_j})$ para toda $j < i$, y $y_i = f(x_{k_i})$. Entonces $f(X) = \{y_0, y_1, \ldots, y_{m-1}\}$ para algún $m \leq n$. ■

Como una consecuencia, si $(a_i)_{i=0}^{n-1}$ es una sucesión (inyectiva o no), entonces el conjunto $\{a_i : i < n\}$ es finito.

Cuando fue necesario mostrar un conjunto infinito (el conjunto de todos los números naturales), agregamos un axioma que garantizara su existencia. Todas las posibles construcciones creadas por el Axioma Esquema de Comprensión, al ser aplicadas a conjuntos finitos, generan conjuntos finitos. Ahora mostraremos que si X es un conjunto finito, entonces $\mathcal{P}(X)$ es finito, y si X es un sistema finito de conjuntos finitos, entonces $\bigcup X$ es finito. Por lo tanto, es necesario agregar el Axioma de Infinitud.

Lema 7.6 *Si X y Y son conjuntos finitos, entonces $X \cup Y$ es finito. Más aún, $|X \cup Y| \leq |X| + |Y|$, y si $X \cap Y = \emptyset$, entonces $|X \cup Y| = |X| + |Y|$.*

Es fácil probar la primera parte del lema, solamente construya una sucesión con rango $X \cup Y$. Para la segunda parte use inducción.

Teorema 7.7 *Si $\mathcal{S}$ es finito y si cualquier $X \in S$ es finito, entonces $\bigcup \mathcal{S}$ es finito.*

Demostración:

Procederemos por inducción sobre el número de elementos de $\mathcal{S}$. La proposición es cierta si $|\mathcal{S}| = 0$. Así, supongamos que es cierta para todo $\mathcal{S}$ con $|\mathcal{S}| = n$ y sea $\mathcal{S} = \{X_0, X_1, \ldots, X_{n-1}, X_n\}$ un conjunto con $n+1$ elementos, con cada $X_i \in \mathcal{S}$ finito. Por la hipótesis de inducción, $\bigcup_{i=0}^{n-1} X_i$ es finito. Como

$$\bigcup \mathcal{S} = \left(\bigcup_{i=0}^{n-1} X_i \right) \cup X_n,$$

por el Lema 7.6, $\bigcup \mathcal{S}$ es finito. ■

Teorema 7.8 *Si X es finito, entonces $\mathcal{P}(X)$ es finito.*

Demostración:

Por inducción sobre $\#(X)$. Si $\#(X) = 0$, entonces $\mathcal{P}(X) = \{\emptyset\}$ es finito. Supongamos que $\mathcal{P}(X)$ es finito cuando $\#(X) = n$, y sea Y un conjunto con $n+1$ elementos:

$$Y = \{y_0, y_1, \ldots, y_n\}.$$

Sea $X = Y \setminus \{y_n\}$. Note que $\mathcal{P}(Y) = \mathcal{P}(X) \cup \mathcal{U}$, donde

$$\mathcal{U} = \{U \in \mathcal{P}(Y) : y_n \in U\}.$$

Además, observe que $\#(\mathcal{U}) = \#(\mathcal{P}(X))$ (puesto que una biyección es $f(U) = U \setminus \{y_n\}$, para todo $U \in \mathcal{U}$). Por lo tanto, $\mathcal{P}(Y)$ es unión de dos conjuntos finitos y así finito. ■

Para concluir esta sección, discutiremos brevemente otro enfoque de la finitud. En la introducción del Capítulo 5 mencionamos que es posible dar una definición de conjunto finito sin hacer referencia a los números naturales. Aquí hay una de tales definiciones: Un conjunto X es *finito* si existe una relación $\preceq$ sobre X tal que

(a) $\preceq$ es un orden lineal en X,

(b) todo subconjunto no vacío de X tiene elementos máximo y mínimo en el orden $\preceq$.

Esta definición de finitud coincide con la que usamos por medio de sucesiones finitas: Si $X = \{x_0, x_1, \ldots, x_{n-1}\}$, entonces $x_0 \preceq x_1 \preceq \cdots \preceq x_{n-1}$ describe un orden lineal en X con las propiedades requeridas. Por otro lado, si $(X, \preceq)$ satisface (a) y (b), construimos, por recursión, una sucesión finita $(x_0, x_1, \ldots)$ como en el Teorema 5.18. La sucesión agota todos los elementos de X, de otro modo el conjunto infinito $\{x_0, x_1, \ldots\}$ no tiene elemento máximo en X.

Mencionemos otra definición de finitud que no involucra a los números naturales. Decimos que un conjunto X es *finito* si cualquier familia no vacía de subconjuntos de X tiene un elemento $\subseteq$-maximal, es decir, si $\emptyset \neq \mathcal{U} \subseteq \mathcal{P}(X)$, entonces existe $U \in \mathcal{U}$ tal que para ningún $V \in \mathcal{U}$, $U \subset V$. En el Ejercicio 7.2.7 se sugiere cómo demostrar la equivalencia de esta definición con la Definición 7.1.

Una última consideración: Se muestra a partir del Lema 7.2 que si X es finito, entonces no hay una función biyectiva de X en un subconjunto propio. Por otro lado, para conjuntos infinitos, como el de los números naturales, existen funciones biyectivas sobre subconjuntos propios (por ejemplo, $f(n) = n + 1$). Si uno define a los conjuntos finitos como aquellos conjuntos que no son equipotentes con algún subconjunto propio, entonces sin el Axioma de Elección es imposible probar la equivalencia de esta definición con la dada en 7.1.

Ejercicios 7.2

1. Pruebe que $m \leq n$ en el Teorema 7.4 (Sugerencia: aplique inducción, $k_i \geq i$ siempre que esté definido, así en particular, $m - 1 \leq k_{m-1} \leq m$.)

2. Sean $A \neq \emptyset$ y $n \in \mathbf{N}$. Demuestre que son equivalentes:

   (a) Existe $f : n \to A$ sobreyectiva.

   (b) Existe $g : A \to n$ inyectiva.

   (c) A es finito con a lo más n elementos.

3. Pruebe que si X, Y son conjuntos finitos entonces $X \times Y$ es un conjunto finito y $\#(X \times Y) = \#(X) \cdot \#(Y)$.

4. Demuestre el Lema 7.6.

5. Pruebe que si X tiene n elementos entonces $\mathcal{P}(X)$ tiene 2^n elementos.

6. Demuestre que si X, Y son conjuntos finitos entonces X^Y tiene $|X|^{|Y|}$ elementos.

7. Demuestre que X es finito si y sólo si cualquier familia no vacía de subconjuntos de X tiene un elemento $\subseteq$-maximal. (Sugerencia: sea $|X| = n$ y $\mathcal{U} \subseteq \mathcal{P}(X)$. Sea m el máximo número en $\{|U| : U \in \mathcal{U}\}$. Si $U \in \mathcal{U}$ y $|U| = m$, entonces U es maximal. Por otro lado, si X es infinito, sea $\mathcal{U} = \{Y \subseteq X : Y \text{ es finito}\}$.)

8. Use el Lema 7.2 y los Ejercicios 3 y 6 para dar demostraciones fáciles de la conmutatividad y asociatividad de la suma y multiplicación de números naturales, distribución de la multiplicación sobre la suma, y las propiedades usuales de la exponenciación.

9. Pruebe que si X es finito y $\preceq$, $\trianglelefteq$ son dos ordenes totales para X, entonces $(X, \preceq)$ y $(X, \trianglelefteq)$ son isomorfos.

10. Sea $R \subseteq A^2$ un buen orden. Muestre que salvo que A sea finito, R^{-1} no es un buen orden.

7.3 Cardinalidad en Conjuntos Infinitos

En el Capítulo 5 dimos una definición precisa de la proposición "los conjuntos A y B tienen la misma cantidad de elementos". Afirmamos que los conjuntos A y B *tienen la misma cardinalidad* si existe una función biyectiva de A en B. En la sección anterior pusimos nuestra atención a los conjuntos finitos y probamos algunas de sus propiedades; ahora empezaremos a investigar propiedades de los conjuntos infinitos. Una definición propia del conjunto $|X|$, el "número" de elementos del conjunto X, es técnicamente difícil, por lo tanto, la pospondremos para el Capítulo 9 y nos concentraremos, en la presente sección, en la propiedad "A y B tienen la misma cardinalidad". Empezamos con la siguiente definición.

Definición 7.9 La *cardinalidad de A es menor o igual a la cardinalidad de B,* si existe una función inyectiva de A en B.

A pesar de que los objetos $|A|$ y $|B|$ no hayan sido definidos, es conveniente usar la notación $|A| = |B|$ para expresar "A y B tienen la misma cardinalidad" y $|A| \leq |B|$ para "la cardinalidad de A es menor o igual a la cardinalidad de B". Cuando se defina con precisión el símbolo $|X|$, mostraremos que la notación es consistente con la presente notación, es decir, que A y B son equipotentes

si y sólo si $|A|$ es el mismo conjunto que $|B|$, etc. El lector puede notar que para conjuntos finitos A y B esto es una consecuencia de la Definición 7.1 y del Corolario 7.3.

Algunas propiedades importantes son:

(a) Si $|X| = |Y|$, entonces $|X| \leq |Y|$ y $|Y| \leq |X|$.

(b) Si $|X| \leq |Y|$ y $|Y| \leq |Z|$, entonces $|X| \leq |Z|$. En efecto si $f : X \to Y$ y $g : Y \to Z$ son funciones inyectivas, entonces $g \circ f : X \to Z$ es inyectiva.

(c) Si $|X| \leq |Y|$ y $|Y| \leq |X|$, entonces $|X| = |Y|$. Esto es mucho menos trivial y posponemos la demostración hasta la Sección 7.5.

Así, la propiedad $|X| = |Y|$ es una (clase) relación de equivalencia y $|X| \leq |Y|$ es un orden parcial en la clase de los conjuntos. Una pregunta natural es cuándo esta relación es un (clase) orden total, es decir, cuándo

(d) $|X| \leq |Y|$ o $|Y| \leq |X|$ se cumple para todo X, Y.

Se sabe que esto no puede demostrarse sin el Axioma de Elección, por ello lo posponemos para el Capítulo 9.

Decimos que *la cardinalidad de X es menor que la cardinalidad de Y* y escribimos $|X| < |Y|$ si $|X| \leq |Y|$, pero la relación $|X| = |Y|$ no se cumple; esto es, si existe una función inyectiva de X en Y y no existe una biyección. Note que esto no equivale a decir: Existe una función inyectiva de X en Y, pero no sobre Y.

Teorema 7.10 *Si X es infinito, entonces $|X| > |n|$ para todo $n \in \mathbf{N}$.*

Demostración:

Es suficiente mostrar que $|X| \geq |n|$ para todo $n \in \mathbf{N}$, lo cual puede realizarse por inducción. Claramente, $|0| \leq |X|$. Supongamos que $|X| \geq |n|$; entonces hay una función inyectiva $f : n \to X$. Como X es infinito, existe $x \in X \setminus ran\, f$. Definamos $g = f \cup \{(n, x)\}$; $g : n + 1 \to X$ es inyectiva. Por lo tanto, $|X| \geq |n + 1|$. ■

Ejercicios 7.3

1. Muestre que:

   (a) Si $|X| = |Y|$ y $|Y| \leq |Z|$, entonces $|X| \leq |Z|$.

   (b) Si $|X| \leq |Y|$ y $|Y| < |Z|$, entonces $|X| < |Z|$.

2. Sea S un conjunto, y sea $\mathcal{F}$ el conjunto de todos los subconjuntos finitos de S. Demuestre que $|S| \leq |\mathcal{F}| \leq |\mathcal{P}(S)|$. (Sugerencia: $|S| = |\{\{a\} : a \in S\}|$.)

3. Muestre que $|A| \leq \left|A^S\right|$ para cualquier A y cualquier $S \neq \emptyset$.

4. Demuestre que $|T| \leq \left|S^T\right|$ si $|S| \geq |2|$. (Sugerencia: fije $u, v \in S$ y para cada $t \in T$, considere $f_t : T \to S$ tal que $f_t(t) = u$, $f_t(x) = v$ de otro modo.)

5. Demuestre que:

   (a) Cualesquiera dos intervalos abiertos de números reales (a, b) y (c, d) son equipotentes.

   (b) $\mathbf{R}$ es equipotente a $(0, 1)$.

7.4 Conjuntos Numerables

El Axioma de Infinitud nos provee de un conjunto infinito (el conjunto de los números naturales) del cual se desprenden muchos otros conjuntos infinitos. En esta sección investigaremos la cardinalidad de $\mathbf{N}$, esto es, estamos interesados en conjuntos equipotentes al conjunto $\mathbf{N}$.

Definición 7.11 (a) Un conjunto S es *numerable* si $|S| = |\mathbf{N}|$.
(b) Un conjunto es *a lo más numerable* si $|S| \leq |\mathbf{N}|$.

Así, un conjunto S es numerable si y sólo si existe una biyección de $\mathbf{N}$ en S; S es a lo más numerable si existe una función inyectiva de S en $\mathbf{N}$.

Ejemplo 7.12 Tanto el conjunto de los números naturales pares como el conjunto de números naturales impares son numerables, a pesar de ser subconjuntos propios de $\mathbf{N}$.

Teorema 7.13 *Un subconjunto infinito de un conjunto numerable es numerable.*

Demostración:

Sea A un conjunto numerable, y sea $B \subseteq A$ infinito. Entonces hay una sucesión inyectiva $(a_n)_{n=0}^{\infty}$ cuyo rango es A. Sea $b_0 = a_{k_0}$, donde k_0 es el mínimo k tal que $a_k \in B$. Teniendo construido b_n, sea $b_{n+1} = a_{k_{n+1}}$, donde k_{n+1} es el mínimo k tal que $a_k \in B$ y $a_k \neq b_i$ para todo $i \leq n$. Tal k existe puesto que

B es infinito. La existencia de la sucesión $(b_n)_{n=0}^{\infty}$ se sigue fácilmente por el Teorema de Recursión 5.17. Es fácil ver (por inducción) que $B = \{b_n : n \in \mathbf{N}\}$ y que $(b_n)_{n=0}^{\infty}$ es inyectiva. Así, B es numerable. ■

Ejemplo 7.14 El conjunto de los números primos es numerable. Obsérvese que esto implica la existencia de una función biyectiva del conjunto de los números naturales en el conjunto de los números primos.

Si un conjunto S es a lo más numerable, entonces es equipotente a un subconjunto de un conjunto numerable; por el Teorema 7.13, éste es o bien finito o numerable. Así tenemos el siguiente corolario.

Corolario 7.15 *Un conjunto es a lo más numerable si y sólo si es o bien finito o numerable.*

El rango de una sucesión inyectiva es numerable. Si $(a_n)_{n=0}^{\infty}$ es una sucesión la cual no es inyectiva, entonces el conjunto $\{a_n : n \in \mathbf{N}\}$ puede ser finito (por ejemplo, si la sucesión es constante). Sin embargo si el rango es infinito, entonces es numerable.

Teorema 7.16 *El rango de una sucesión $(a_n)_{n=0}^{\infty}$ es a lo más numerable; es decir, finito o numerable. En otras palabras la imagen de un conjunto numerable bajo una función es a lo más numerable.*

Demostración:

Por recursión construiremos una sucesión (b_n) (con dominio finito o infinito) la cual es inyectiva y tiene el mismo rango que $(a_n)_{n=0}^{\infty}$. Sea $b_0 = a_0$, y teniendo construido b_n, sea $b_{n+1} = a_{k_{n+1}}$, donde k_{n+1} es el mínimo k tal que $a_k \neq b_i$ para toda $i \leq n$. (Si no hay tales k, entonces consideramos la sucesión finita $(b_i)_{i<n+1}$.) La sucesión $(b_n)_{n=0}^{\infty}$ así construida es inyectiva y su rango es $\{a_n : n \in \mathbf{N}\}$. ■

Nótese que una diferencia entre los conjuntos finitos e infinitos es la siguiente: Si S es un conjunto numerable entonces S puede descomponerse en dos partes ajenas, A y B, tales que $|A| = |B| = |S|$, que es inconcebible si S es finito (salvo $S = \emptyset$). Podemos de hecho hacer algo más. Sea p_n el n-ésimo número primo y sean

$$S_n = \left\{ p_n^k : k \in \mathbf{N} \right\}.$$

Los conjuntos S_n $(n \in \mathbf{N})$ son ajenos por pares e infinitos. Así tenemos que $\mathbf{N} \supseteq \bigcup_{n=0}^{\infty} S_n$ con $|S_n| = |\mathbf{N}|$.

Los siguientes dos teoremas muestran que las operaciones simples aplicadas a conjuntos numerables generan conjuntos numerables.

Teorema 7.17 *La unión de dos conjuntos numerables es un conjunto numerable.*

DEMOSTRACIÓN:

Sean $A = \{a_n : n \in \mathbf{N}\}$ y $B = \{b_n : n \in \mathbf{N}\}$, entonces basta construir una sucesión $(c_n)_{n=0}^{\infty}$ como sigue:

$$c_{2k} = a_k \quad \text{y} \quad c_{2k+1} = b_k$$

para todo $k \in \mathbf{N}$. Ahora, $A \cup B = \{c_n : n \in \mathbf{N}\}$ y como es un conjunto infinito, es entonces numerable. ■

Corolario 7.18 *La unión de una familia finita de conjuntos numerables es un conjunto numerable.*

Uno puede conjeturar que es posible establecer un resultado más fuerte, es decir, demostrar que la unión de una familia numerable de conjuntos numerables es un conjunto numerable. Sin embargo, esto puede probarse solamente usando el Axioma de Elección; de hecho, sin usar el Axioma de Elección no se puede demostrar el siguiente teorema "evidente". Si $\mathcal{A} = \{A_n : n \in \mathbf{N}\}$ y $|A_n| = 2$ para cada n, entonces $\bigcup_{n=0}^{\infty} A_n$ es numerable. (Compare esto con los Ejercicios 7.4.11 y 7.4.12.)

Teorema 7.19 *Si A y B son conjuntos numerables, entonces $A \times B$ es numerable.*

DEMOSTRACIÓN:

Es suficiente mostrar que $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$ (ver Ejercicio 7.4.2.)

Consideremos la función $f : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ dada por

$$f(m, n) = 2^m(2n + 1) - 1.$$

Se le pide al lector verificar que esta función es biyectiva. ■

Corolario 7.20 *El producto cartesiano de una cantidad finita de conjuntos numerables es numerable. Consecuentemente, $\mathbf{N}^m$ es numerable para todo $m \in \mathbf{N}$.*

Corolario 7.21 *El conjunto de los números enteros $\mathbf{Z}$ y el conjunto de los números racionales $\mathbf{Q}$ son numerables.*

DEMOSTRACIÓN:

Por el Teorema 7.17, $\mathbf{Z}$ y $\mathbf{Z}\backslash\{0\}$ son numerables, así que el conjunto de cocientes $\mathbf{Z}\times\mathbf{Z}\backslash\{0\}$ es numerable, y puesto que la proyección natural de $\mathbf{Z}\times\mathbf{Z}\backslash\{0\}$ en $\mathbf{Q}$ es sobreyectiva, por el Teorema 7.16, $\mathbf{Q}$ es numerable. ■

Para que no pensemos que todos los conjuntos infinitos son numerables, he aquí un importante ejemplo de un conjunto no numerable.

Teorema 7.22 *El conjunto de los números reales* $\mathbf{R}$ *es un conjunto no numerable.*

DEMOSTRACIÓN:

Tomemos una sucesión cualquiera de números reales $(a_n)_{n=0}^{\infty}$. Expresemos cada número real a_n en su expansión decimal (ver Teorema 6.48):

$$a_0 = a_0^{(0)}.\, a_1^{(0)} a_2^{(0)} a_3^{(0)} \cdots$$

$$a_1 = a_0^{(1)}.\, a_1^{(1)} a_2^{(1)} a_3^{(1)} \cdots$$

$$a_2 = a_0^{(2)}.\, a_1^{(2)} a_2^{(2)} a_3^{(2)} \cdots$$
$$\cdots$$

Sea $b = b_0.\, b_1 b_2 b_3 \cdots$ el número real definido como sigue:

$$b_n = \begin{cases} 0, & \text{si } a_n^{(n)} \neq 0 \\ 1, & \text{si } a_n^{(n)} = 0. \end{cases}$$

Entonces $b \neq a_n$ para cada n y así b no pertenece al rango de la sucesión $(a_n)_{n=0}^{\infty}$, lo cual implica que no existen sucesiones sobreyectivas de números reales. Por lo tanto, $|\mathbf{N}| < |\mathbf{R}|$; así, $\mathbf{R}$ no es numerable. ■

Este resultado, original de Cantor, despertó en su momento una gran controversia; de él se concluye que existen diferentes "tamaños" de conjuntos infinitos.

Ejercicios 7.4

1. Sea A un conjunto numerable y $x \in A$, muestre que $A \setminus \{x\}$ es numerable; concluya que un conjunto numerable siempre es equipotente a un subconjunto propio.

2. Pruebe que si $|A_1| = |A_2|$ y $|B_1| = |B_2|$, entonces $|A_1 \times B_1| = |A_2 \times B_2|$.

3. Pruebe que la función f en la demostración del Teorema 7.19 es biyectiva.

4. Un número real x es *algebraico* si es solución de alguna ecuación

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

donde los a_i son números enteros. Si x no es algebraico se llama *trascendental*.

   (a) Muestre que el conjunto de números algebraicos es numerable.

   (b) Muestre que el conjunto de números trascendentales es no numerable.

5. Pruebe que el conjunto de todas las líneas rectas del plano $\mathbf{R}^2$ que pasan por al menos dos puntos con coordenadas racionales es numerable.

6. Para cada $n \neq 0$, demuestre que el conjunto

$$[\mathbf{N}]^n = \{S \subseteq \mathbf{N} : |S| = n\}$$

es numerable. (Sugerencia: $[\mathbf{N}]^n$ es la imagen de un conjunto numerable.)

7. Sea $\mathcal{S}$ el conjunto de todas las sucesiones semiconstantes de números naturales ($(s_n)_{n=0}^{\infty}$ es semiconstante si existe $n_0 \in \mathbf{N}$ tal que para todo $n \geq n_0$, $s_n = s_{n_0}$). Demuestre que $\mathcal{S}$ es numerable. (Sugerencia: para $s \in \mathcal{S}$ sea $f(s) = \prod_{i<n_0} p_i^{s_i}$, donde p_i es el i-ésimo número primo. La función f es inyectiva.)

8. Pruebe que el conjunto de todas las sucesiones finitas de números naturales es numerable. Después observaremos que el paso a todas las sucesiones de números naturales no es numerable.

9. Demuestre que el conjunto de todos los subconjuntos finitos de números naturales es numerable. (Use el Ejercicio 8 y el Teorema 7.16.)

10. Sea S un conjunto numerable y R una relación de equivalencia en S. Muestre que:

    (a) El conjunto S/R es a lo más numerable.

    (b) Dé un ejemplo en el cual S/R sea finito.

11. Sea $\{A_n : n \in \mathbf{N}\}$ una familia numerable, y supóngase que se tiene una sucesión $(a_n)_{n=0}^{\infty}$ de enumeraciones de los conjuntos A_n; esto es, $a_n = (a_{n,k})_{k=0}^{\infty}$ y $A_n = \{a_{n,k} : k \in \mathbf{N}\}$ para cada $n \in \mathbf{N}$. Demuestre que $\bigcup_{n=0}^{\infty} A_n$ es numerable.

12. Sea $(S, \leq)$ un conjunto linealmente ordenado. Sea $\{A_n : n \in \mathbf{N}\}$ un sistema numerable de conjuntos finitos de S. Demuestre que $\bigcup_{n=0}^{\infty} A_n$ es numerable. (Sugerencia: para todo n, considere la única enumeración $(a_{n,k})_{k<|A_n|}$ de A_n en el orden creciente: $a_{n,0} < a_{n,1} < \cdots < a_{n,k_{n-1}}$ donde $k_n = |A_n|$.)

13. (a) Sean A, B y C conjuntos tales que $C \subseteq A$, $A \cap B = \emptyset$, y B y C numerables. Pruebe que $|A \cup B| = |A|$.

    (b) Pruebe que un conjunto que contiene un subconjunto numerable es equipotente a la unión del conjunto y un conjunto numerable.

    (c) Pruebe que si A es no numerable y B es numerable, entonces $A \setminus B$ es no numerable.

7.5 Números Cardinales

En la Sección 3 usamos el símbolo $|A|$ sin hacer una definición formal de éste. Para lo que sigue es más conveniente tener al símbolo $|A|$ como un objeto de la Teoría de Conjuntos. Por esta razón hacemos la siguiente suposición.

Suposición 7.23 Existen conjuntos llamados números cardinales (o cardinales) con la propiedad de que para cualquier conjunto X, hay un único cardinal $|X|$ (el número cardinal de X), y para cualesquiera conjuntos X y Y, son equipotentes si y sólo si $|X|$ es igual a $|Y|$.

También en la Sección 3 vimos que la relación $|X| \leq |Y|$ es un orden parcial en la ahora clase de los números cardinales, pero prometimos probar en esta sección que si $|X| \leq |Y|$ y $|Y| \leq |X|$, entonces $|X| = |Y|$; para ello necesitamos del siguiente lema.

Lema 7.24 *Si $A_1 \subseteq B \subseteq A$ y $|A_1| = |A|$, entonces $|B| = |A|$.*

DEMOSTRACIÓN:

Sea $f : A \to A_1$ una función biyectiva. Por recursión, definamos dos sucesiones de conjuntos

$$A_0,\ A_1,\ \ldots,\ A_n, \ldots$$

y

$$B_0,\ B_1,\ \ldots,\ B_n, \ldots$$

Sean

$$A_0 = A \quad \text{y} \quad B_0 = B$$

y para cada $n \in \mathbf{N}$,

$$A_{n+1} = f(A_n), \qquad B_{n+1} = f(B_n). \tag{7.5.1}$$

Como $A_0 \supseteq B_0 \supseteq A_1$, se sigue de (7.5.1), por inducción, que para toda $n \in \mathbf{N}$, $A_n \supseteq B_n \supseteq A_{n+1}$. Para cada $n \in \mathbf{N}$, sea $C_n = A_n \setminus B_n$ y

$$C = \bigcup_{n=0}^{\infty} C_n, \qquad D = A \setminus C$$

Por (7.5.1) y el hecho de que f es una función inyectiva, tenemos que $f(C_n) = C_{n+1}$; así,

$$f(C) = \bigcup_{n=1}^{\infty} C_n.$$

Ahora definamos $g : A \to B$ como sigue:

$$g(x) = \begin{cases} f(x), & \text{si } x \in C \\ x, & \text{si } x \in D. \end{cases}$$

Como $g\,|_C$ y $g\,|_D$ son funciones inyectivas y sus rangos son ajenos, se concluye que g es una función inyectiva de A sobre $f(C) \cup D = B$. ■

Teorema 7.25 (Cantor-Schröder-Bernstein) *Si A y B son conjuntos tales que $|A| \leq |B|$ y $|B| \leq |A|$, entonces $|A| = |B|$.*

DEMOSTRACIÓN:

Si $|A| \leq |B|$, entonces existe una función inyectiva $f : A \to B$, y como $|B| \leq |A|$, existe $g : B \to A$ inyectiva. La función $g \circ f : A \to A$ es inyectiva y $|A| = |g \circ f(A)|$; además, $g \circ f(A) \subseteq g(B) \subseteq A$. Luego, $|g(B)| = |A|$. Por otro lado, $|B| = |g(B)|$. Concluimos que $|A| = |B|$. ■

Ahora demostraremos el resultado principal de esta sección, el célebre *Teorema "Diagonal" de Cantor*, en su forma más abstracta.

Teorema 7.26 (Cantor) *Para todo conjunto A se tiene:*

$$|A| < |\mathcal{P}(A)|\,.$$

Demostración:

Si $A = \emptyset$, entonces $\mathcal{P}(A) = \{\emptyset\}$ y así $|A| < |\mathcal{P}(A)|$. Si $A \neq \emptyset$, es claro que la función

$$x \mapsto \{x\}$$

es inyectiva, con lo cual $|A| \leq |\mathcal{P}(A)|$. Por otra parte, si $f : A \to \mathcal{P}(A)$ es cualquier función, entonces el conjunto

$$S = \{x \in A : x \notin f(x)\}$$

no está en el rango de f, de aquí que f no puede ser sobreyectiva. Por lo tanto, $|A| < |\mathcal{P}(A)|$. ■

La importancia del Teorema de Cantor es que establece que para cualquier cardinal $|X|$ hay un cardinal estrictamente mayor, $|\mathcal{P}(X)|\,$.

Concluimos esta sección, pequeña pero importante, con otro resultado sobre números cardinales.

Teorema 7.27 *Sea $\mathcal{F}$ una familia de conjuntos tal que no hay un cardinal maximal entre los cardinales de los miembros de $\mathcal{F}$; en otras palabras, si $X \in \mathcal{F}$, entonces existe $Y \in \mathcal{F}$ tal que $|X| < |Y|$. Entonces $\bigcup \mathcal{F}$ tiene cardinalidad mayor que cualquier conjunto en $\mathcal{F}$.*

Demostración:

Sea $S = \bigcup \mathcal{F}$. Claramente $|X| \leq |S|$ para cada $X \in \mathcal{F}$. Mostraremos que no hay un $X \in \mathcal{F}$ tal que $|S| \leq |X|$. Supongamos lo contrario, sea $X \in \mathcal{F}$ con $|S| \leq |X|$, entonces por hipótesis existe $Y \in \mathcal{F}$ tal que $|X| < |Y|$. Como $|Y| \leq |S|$, tenemos que $|Y| \leq |X|$, lo cual es una contradicción. ■

Ejercicios 7.5

1. Use el Teorema de Cantor para mostrar que la clase de todos los conjuntos no es un conjunto.

2. (a) Usando el Teorema de Cantor-Schröder-Bernstein, demuestre que cualquier conjunto abierto de números reales tiene la misma cardinalidad que $\mathbf{R}$. (Sugerencia: Un conjunto abierto de números reales es la unión de una familia de intervalos abiertos.)
   (b) Muestre que cualquier intervalo abierto contiene números irracionales.

3. Sea X un conjunto y supóngase que $f : X \to X$ es una función inyectiva. Demuestre que X es infinito.

4. Un conjunto X se llama *infinito según Dedekind* si existe una función inyectiva $f : X \to X$. Un conjunto es *finito según Dedekind* si no es infinito según Dedekind.

   (a) Muestre que todo conjunto numerable es infinito según Dedekind.
   (b) Muestre que si X es un conjunto que contiene un subconjunto numerable entonces es infinito según Dedekind.
   (c) Si X es un conjunto infinito según Dedekind, entonces contiene un subconjunto numerable. (Sugerencia: sea $x \in X \setminus f(X)$, y defina $x_{n+1} = f(x_n)$.) Así, los conjuntos infinitos según Dedekind son precisamente los que tienen subconjuntos numerables. Usando el Axioma de Elección después se verá que "infinito" es equivalente a "infinito según Dedekind".

5. Sean A y B conjuntos infinitos según Dedekind. Muestre que $A \cup B$ y $A \times B$ también son conjuntos infinitos según Dedekind.

6. Pruebe que si A es un conjunto infinito, entonces $\mathcal{P}(\mathcal{P}(A))$ es infinito según Dedekind. (Sugerencia: para cada $n \in \mathbf{N}$, sea

$$S_n = \{X \subset A : |X| = n\}.$$

   El conjunto $\{S_n : n \in \mathbf{N}\}$ es numerable.)

7.6 Aritmética Cardinal

En esta sección definiremos operaciones aritméticas (suma, multiplicación y exponenciación) de números cardinales e investigaremos sus propiedades.

Para definir la suma $\kappa + \lambda$ de dos cardinales usaremos la analogía con los conjuntos finitos: Si A tiene a elementos, B tiene b elementos y $A \cap B = \emptyset$, entonces $A \cup B$ tiene $a + b$ elementos.

Definición 7.28 Si $|A| = \kappa$, $|B| = \lambda$ y $A \cap B = \emptyset$, entonces

$$\kappa + \lambda = |A \cup B|\,.$$

La definición anterior supone que existen conjuntos ajenos A y B tales que $\kappa = |A|$ y $\lambda = |B|$. Esto obviamente es cierto. Por ejemplo tomando $A_1 = A \times \{0\}$ y $B_1 = B \times \{1\}$, entonces $\kappa = |A_1| = |A|$, $\lambda = |B_1| = |B|$ y $A_1 \cap B_1 = \emptyset$. También, para hacer legítima esta definición debemos mostrar que $\kappa+\lambda$ no depende de la elección de los conjuntos A y B. Esto está contenido en el siguiente lema.

Lema 7.29 *Si A, B, A', B' son tales que $|A| = |A'|$, $|B| = |B'|$ y $A \cap B = \emptyset = A' \cap B'$, entonces $|A \cup B| = |A' \cup B'|$.*

Demostración:

Sean $f : A \to A'$ y $g = B \to B'$ funciones biyectivas. Entonces $f \cup g : A \cup B \to A' \cup B'$ es biyectiva. ■

No solamente la suma de cardinales coincide con la suma ordinaria de números en el caso finito, también se preservan algunas de las propiedades usuales. Por ejemplo, la suma de números cardinales es conmutativa y asociativa:

(a) $\kappa + \lambda = \lambda + \kappa$.
(b) $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$.

Estas propiedades se siguen directamente de la definición. Similarmente las siguientes desigualdades se establecen con facilidad.

(c) $\kappa \leq \kappa + \lambda$
(d) Si $\kappa_1 \leq \kappa_2$ y $\lambda_1 \leq \lambda_2$, entonces $\kappa_1 + \lambda_1 \leq \kappa_2 + \lambda_2$.

Sin embargo, no todas las propiedades de la suma de números naturales son válidas para la suma de cardinales. En particular, las desigualdades estrictas son raras en el caso de cardinales infinitos y, como será discutido después (Teorema de König), las que son válidas resultan difíciles de establecer. Como un ejemplo, tenemos el hecho de que si $n \neq 0$, entonces $n + n > n$; por el contrario, si κ es infinito, el Axioma de Elección implica que $\kappa + \kappa = \kappa$. Ya hemos visto que $|\mathbf{N}| + |\mathbf{N}| = |\mathbf{N}|$.

La multiplicación de cardinales está nuevamente motivada por las propiedades de la multiplicación de números naturales. Si A y B son conjuntos de a y b elementos, respectivamente, entonces $A \times B$ tiene $a \cdot b$ elementos.

Definición 7.30 Si $|A| = \kappa$ y $|B| = \lambda$, entonces

$$\kappa \cdot \lambda = |A \times B| .$$

Lema 7.31 *Si A, B, A', B' son tales que $|A| = |A'|$ y $|B| = |B'|$, entonces $|A \times B| = |A' \times B'|$.*

DEMOSTRACIÓN:

Sean $f : A \to A'$ y $g : B \to B'$ funciones, definamos $h : A \times B \to A' \times B'$ por

$$h(a, b) = (f(a), g(b)) .$$

Claramente si f y g son funciones biyectivas, también lo es h. ■

Este lema garantiza que la definición de multiplicación no depende de la elección de los conjuntos A y B.

Nuevamente la multiplicación tiene algunas propiedades esperadas; en particular, ésta es conmutativa y asociativa. Más aún, también se tiene la distribución sobre la suma.

(e) $\kappa \cdot \lambda = \lambda \cdot \kappa$.
(f) $\kappa \cdot (\lambda \cdot \mu) = (\kappa \cdot \lambda) \cdot \mu$.
(g) $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$.

La última de las propiedades es una consecuencia de la igualdad

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

que se cumple para cualesquiera conjuntos A, B y C. También tenemos:

(h) $\kappa \leq \kappa \cdot \lambda$ si $\lambda > 0$.
(i) Si $\kappa_1 \leq \kappa_2$ y $\lambda_1 \leq \lambda_2$, entonces $\kappa_1 \cdot \lambda_1 \leq \kappa_2 \cdot \lambda_2$.

Para seguir con la analogía probaremos que:

(j) $\kappa + \kappa = 2 \cdot \kappa$.

DEMOSTRACIÓN:

Si $|A| = \kappa$, entonces $2 \cdot \kappa$ es el cardinal de $\{0,1\} \times A$. Notemos que

$$\{0,1\} \times A = (\{0\} \times A) \cup (\{1\} \times A),$$

$|\{0\} \times A| = |\{1\} \times A| = \kappa$ y que los sumandos son ajenos. Por lo tanto, $\kappa + \kappa = 2 \cdot \kappa$. ■

Como una consecuencia de *(j)* tenemos:

(k) $\kappa + \kappa \leq \kappa \cdot \kappa$ si $\kappa \geq 2$.

Como en el caso de la suma, la multiplicación de cardinales infinitos tiene algunas propiedades que difieren de las correspondientes para los números naturales. Por ejemplo, $|\mathbf{N}| \cdot |\mathbf{N}| = |\mathbf{N}|$.

Para definir la exponenciación de números cardinales observemos que si A y B son conjuntos finitos no ambos vacíos, con a y b elementos respectivamente, entonces a^b es el número de todas las funciones de B en A.

Definición 7.32 Si $|A| = \kappa$ y $|B| = \lambda$, entonces

$$\kappa^\lambda = \left|A^B\right|.$$

La definición de κ^λ no depende de la elección de A y B.

Lema 7.33 *Si* $|A| = |A'|$ *y* $|B| = |B'|$, *entonces* $\left|A^B\right| = \left|A'^{B'}\right|$.

DEMOSTRACIÓN:

Sean $f : A \to A'$ y $g : B \to B'$ funciones biyectivas y sea

$$F : A^B \to A'^{B'}$$

definida como sigue: Si $k \in A^B$, sea $F(k) = h$, donde $h : B' \to A'$ es tal que $h(g(b)) = f(k(b))$ para todo $b \in B$. Entonces F es una biyección. ■

Es fácil ver desde la definición de exponenciación que:

(l) $\kappa \leq \kappa^\lambda$ si $\lambda > 0$.
(m) $\lambda \leq \kappa^\lambda$ si $\kappa > 1$.
(n) Si $\kappa_1 \leq \kappa_2$ y $\lambda_1 \leq \lambda_2$, entonces $\kappa_1^{\lambda_1} \leq \kappa_2^{\lambda_2}$.

También tenemos:

(ñ) $\kappa \cdot \kappa = \kappa^2$

Para probar *(ñ)*, es suficiente tener una correspondencia entre $A \times A$ y el conjunto de funciones de $\{0,1\}$ en A. Esto se estableció en el Ejemplo 4.58.

El siguiente teorema establece otras propiedades de la exponenciación.

Teorema 7.34 *(a)* $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$.
(b) $(\kappa^\lambda)^\mu = \kappa^{\lambda\cdot\mu}$.

DEMOSTRACIÓN:

(a) Sean $\kappa = |K|$, $\lambda = |L|$, $\mu = |M|$ con $L \cap M = \emptyset$. Construiremos una biyección

$$F : K^L \times K^M \to K^{L\cup M}.$$

Si $(f,g) \in K^L \times K^M$, sea $F(f,g) = f \cup g$. Note que $f \cup g$ es una función; de hecho, $f \cup g$ es un miembro de $K^{L\cup M}$. Además, cualquier $h \in K^{L\cup M}$ es igual a $F(f,g)$ para algún $(f,g) \in K^L \times K^M$ (a saber, $f = h \restriction_L$ y $g = h \restriction_M$). Es fácil ver que F es inyectiva.

(b) Ahora construiremos una biyección $F : K^{L\times M} \to (K^L)^M$. Un elemento típico de $K^{L\times M}$ es una función $f : L \times M \to K$. Sea $F(f)$ la función $g : M \to K^L$ definida para cada $m \in M$ por $g(m)(l) = f(l,m)$ para cada $l \in L$. Dejamos al lector que verifique que F es biyectiva. ■

Concluimos esta sección con el siguiente teorema importante.

Teorema 7.35 *Si* $|A| = \kappa$, *entonces* $|\mathcal{P}(A)| = 2^\kappa$.

DEMOSTRACIÓN:

Hay una correspondencia biunívoca entre los subconjuntos de A y las funciones de A en $\{0,1\}$. A cada $B \subseteq A$, le corresponde la función característica de B, χ_B que está definida por

$$\chi_B(x) = \begin{cases} 1, & \text{si } x \in B \\ 0, & \text{si } x \notin B. \end{cases}$$

Es inmediato que si $B \neq C$, entonces $\chi_B \neq \chi_C$ y toda función $f \in \{0,1\}^A$ es la función característica de algún $B \subseteq A$ (de hecho, $B = \{x \in A : f(x) = 1\}$). Por lo tanto, la función $F : \mathcal{P}(A) \to \{0,1\}^A$ definida por $F(B) = \chi_B$ es una biyección entre $\mathcal{P}(A)$ y 2^A. ■

En particular, el Teorema de Cantor ahora tiene la siguiente forma: Para cualquier cardinal κ,

$$\kappa < 2^{\kappa}.$$

Ejercicios 7.6

1. Muestre que $\kappa^0 = 1$ para todo κ y $\kappa^1 = \kappa$ para todo $\kappa > 0$.
2. Muestre que $1^{\kappa} = 1$ para todo κ y $0^{\kappa} = 0$ para todo $\kappa > 0$.
3. Complete la demostración del Teorema 7.34.
4. Pruebe que $\kappa^{\kappa} \leq 2^{\kappa \cdot \kappa}$.
5. Pruebe que si $|A| \leq |B|$ y $A \neq \emptyset$, entonces existe una función sobreyectiva de B en A. Después mostraremos, con ayuda del Axioma de Elección, que el recíproco también es cierto: Si hay una función sobreyectiva de B en A, entonces $|A| \leq |B|$.
6. Demuestre que si existe una función sobreyectiva de B en A, entonces $2^{|A|} \leq 2^{|B|}$. (Sugerencia: Dada una sobreyección $g : B \to A$, sea $f(X) = g^{-1}(X)$ para todo $X \subseteq A$.)
7. ¿Existe un conjunto A tal que $\mathcal{P}(A)$ sea numerable?

7.7 El Continuo

Por el Teorema Diagonal de Cantor, la cardinalidad del conjunto de los números reales es mayor que la cardinalidad del conjunto de los números naturales. En esta sección, analizaremos la cardinalidad de $\mathbf{R}$ y estableceremos algunas propiedades del número cardinal $|\mathbf{R}|$.

Acorde a la Suposición 7.23, hay un conjunto $|\mathbf{N}|$, el número cardinal del conjunto $\mathbf{N}$ (y de todos los conjuntos numerables), el cual denotaremos por[1]

$$\aleph_0.$$

[1] $\aleph$ es la primera letra del alfabeto hebreo. Cantor es responsable del empleo de la notación.

Recordemos que por los resultados de las Secciones 3 y 4, tenemos que

$$n < \aleph_0$$

para cada número natural n, y

$$\aleph_0 + \aleph_0 = \aleph_0$$

$$\aleph_0 \cdot \aleph_0 = \aleph_0.$$

El conjunto $\mathbf{R}$ de todos los números reales, en ocasiones llamado *línea real* o *continuo*, tiene número cardinal mayor que $\aleph_0$. A partir de los resultados conocidos acerca de números cardinales, no es difícil mostrar que la cardinalidad de $\mathbf{R}$ es la misma que la de $\mathcal{P}(\mathbf{N})$.

Teorema 7.36 *El número cardinal del continuo es* $2^{\aleph_0}$.

Demostración:

Una sucesión $x : \mathbf{N} \to \mathbf{Q}$ es un subconjunto de $\mathbf{N} \times \mathbf{Q}$, entonces el conjunto de todas las sucesiones de Cauchy $\mathcal{C}$ está contenido en $\mathcal{P}(\mathbf{N} \times \mathbf{Q})$, por lo que

$$|\mathbf{R}| = |\mathcal{C}/\sim| \leq |\mathcal{C}| \leq |\mathcal{P}(\mathbf{N} \times \mathbf{Q})| = 2^{|\mathbf{N}\times\mathbf{Q}|} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.$$

Por otro lado, $2^{\aleph_0} = 2^{|\mathbf{N}|} = \left|\{0,1\}^{\mathbf{N}}\right| \leq |\mathbf{R}|$. ■

Puesto que hay funciones biyectivas de $\mathbf{R}$ en cualquier intervalo abierto, se sigue que cualquier intervalo abierto tiene la cardinalidad del continuo. Consecuentemente, todo conjunto abierto no vacío de números reales tiene cardinalidad $2^{\aleph_0}$. Uno también puede probar (aunque es más difícil) que cualquier conjunto cerrado de números reales es a lo más numerable o tiene cardinalidad $2^{\aleph_0}$. Una pregunta natural es: ¿Existen conjuntos infinitos de números reales de cardinalidad distinta de $\aleph_0$ y $2^{\aleph_0}$?

La Hipótesis del Continuo *No existe un cardinal* κ *tal que*

$$\aleph_0 < \kappa < 2^{\aleph_0}.$$

La Hipótesis del Continuo fue formulada por Cantor en 1900. D. Hilbert la incluyó como el Problema 1 en su famosa lista de problemas matemáticos importantes. K. Gödel [G_2] en 1939 demostró que la hipótesis del continuo es consistente con los axiomas de la Teoría de Conjuntos; esto es, usando los Axiomas de Zermelo-Fraenkel (incluyendo el Axioma de Elección) no se puede

probar que la Hipótesis del Continuo sea falsa. En 1963, P. J. Cohen [C_4] demostró que la Hipótesis del Continuo es independiente de los axiomas de Zermelo-Fraenkel, es decir, que no se puede deducir usando estos axiomas.

Usando las propiedades de los números cardinales demostradas en las secciones precedentes y las propiedades especiales de $\aleph_0$, podemos obtener algunos resultados acerca del cardinal $2^{\aleph_0}$ y mostrar que muchos conjuntos interesantes tienen esta cardinalidad.

Proposición 7.37 *El conjunto de los números complejos tiene cardinalidad* $2^{\aleph_0}$.

Demostración:

Note que los números complejos pueden ser representados como pares ordenados de números reales y así la cardinalidad del conjunto de los números complejos es $|\mathbf{R} \times \mathbf{R}| = 2^{\aleph_0} \cdot 2^{\aleph_0}$. Ahora el resultado se sigue de:

$$2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0 + \aleph_0} = 2^{\aleph_0}. \blacksquare$$

Proposición 7.38 *El conjunto de todas las sucesiones de números naturales tiene cardinalidad* $2^{\aleph_0}$.

Demostración:

El conjunto $\mathbf{N}^{\mathbf{N}}$ tiene cardinalidad $\aleph_0^{\aleph_0}$. Por un lado,

$$\aleph_0^{\aleph_0} \geq 2^{\aleph_0}$$

(por *(n)* de la Sección 6), y por otro lado,

$$\aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.$$

Por lo tanto, $\left|\mathbf{N}^{\mathbf{N}}\right| = 2^{\aleph_0}$. $\blacksquare$

En conexión a esta proposición, recuerde que el Ejercicio 7.4.7 implica que el conjunto de todas las sucesiones semiconstantes de números naturales es numerable.

Mientras la cardinalidad del conjunto de todas las sucesiones de números naturales es mayor que la cardinalidad de $\mathbf{N}$, encontramos que el conjunto de todas las sucesiones de números reales tiene la misma cardinalidad que $\mathbf{R}$:

$$\left|\mathbf{R}^{\mathbf{N}}\right| = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.$$

En los tres ejemplos anteriores se utilizó la igualdad

$$2^{\aleph_0} + 2^{\aleph_0} = 2^{\aleph_0} \cdot 2^{\aleph_0} = 2^{\aleph_0},$$

la cual puede ser fácilmente derivada, usando el Teorema de Cantor-Schröder-Bernstein, y la igualdad $\aleph_0 \cdot \aleph_0 = \aleph_0$:

$$2^{\aleph_0} \leq 2^{\aleph_0} + 2^{\aleph_0} = 2 \cdot 2^{\aleph_0} \leq 2^{\aleph_0} \cdot 2^{\aleph_0} = (2^{\aleph_0})^2 \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.$$

El número de funciones de $\mathbf{R}$ en $\mathbf{R}$, es decir, la cardinalidad del conjunto $\mathbf{R}^{\mathbf{R}}$, es $2^{\aleph_0 \cdot 2^{\aleph_0}}$, de hecho tenemos:

$$\left|\mathbf{R}^{\mathbf{R}}\right| = (2^{\aleph_0})^{2^{\aleph_0}} = 2^{\aleph_0 \cdot 2^{\aleph_0}} = 2^{2^{\aleph_0}}.$$

Éste es el cardinal del conjunto potencia de $\mathbf{R}$ que por el Teorema de Cantor es mayor que $2^{\aleph_0}$. Sin embargo, el número de funciones continuas es sólo $2^{\aleph_0}$.

Proposición 7.39 *El conjunto de todas las funciones continuas de* $\mathbf{R}$ *en* $\mathbf{R}$ *tiene cardinalidad* $2^{\aleph_0}$.

Demostración:

Usaremos el hecho de que cualquier función continua en $\mathbf{R}$ está determinada por sus valores en un conjunto denso. En particular, por sus valores en el conjunto de los números racionales: Si $f, g : \mathbf{R} \to \mathbf{R}$ son dos funciones continuas tales que para cualquier $r \in \mathbf{Q}$, $f(r) = g(r)$, entonces $f = g$. Sea C el conjunto de todas las funciones continuas de $\mathbf{R}$ en $\mathbf{R}$ y sea $\Psi : C \to \mathbf{R}^{\mathbf{Q}}$ la función definida por $\Psi(f) = f\mid_{\mathbf{Q}}$. Por lo anterior, Ψ es inyectiva y así $|C| \leq \left|\mathbf{R}^{\mathbf{Q}}\right| = 2^{\aleph_0}$. Por otro lado, $|C| \geq 2^{\aleph_0}$ (considere las funciones constantes). ■

El conjunto de todos los números irracionales es no numerable, ya que $\mathbf{R}$ es no numerable y $\mathbf{Q}$ es numerable. En efecto, la cardinalidad del conjunto de los números irracionales es $2^{\aleph_0}$, pero algunos esfuerzos son necesarios para demostrarlo. Aquí establecemos un resultado más general.

Proposición 7.40 *Si* A *es un subconjunto numerable de* $\mathbf{R}$*, entonces*

$$|\mathbf{R} \backslash A| = 2^{\aleph_0}.$$

DEMOSTRACIÓN:

Usaremos el hecho de que $|\mathbf{R}\times\mathbf{R}| = |\mathbf{R}| = 2^{\aleph_0}$, y demostraremos que si $A \subseteq \mathbf{R}\times\mathbf{R}$ es numerable, entonces

$$|(\mathbf{R}\times\mathbf{R}) \setminus A| = 2^{\aleph_0}.$$

Sea $P = dom\, A$ (la proyección de A):

$$P = \{x \in \mathbf{R} : (x,y) \in A \text{ para algún } y\}.$$

Como $|A| = \aleph_0$, tenemos $|P| \leq \aleph_0$. Así, existe $x_0 \in \mathbf{R}\setminus P$. Consecuentemente, el conjunto $X = \{x_0\}\times\mathbf{R}$ es ajeno a A, y por lo tanto, $X \subseteq (\mathbf{R}\times\mathbf{R})\setminus A$. Claramente, $|X| = |\mathbf{R}| = 2^{\aleph_0}$; con lo cual concluimos que

$$|(\mathbf{R}\times\mathbf{R})\setminus A| = 2^{\aleph_0}. \ \blacksquare$$

Ejercicios 7.7

1. Muestre que $\left|\{0,1\}^{\mathbf{N}}\right| \leq |\mathbf{R}|$.
2. Muestre que $(2^{2^{\aleph_0}})^2 = 2^{2^{\aleph_0}}$.
3. Demuestre que la cardinalidad del conjunto de todas las funciones $f : \mathbf{N} \to \{0,1,\ldots,9\}$ es igual a $2^{\aleph_0}$.
4. Demuestre que la cardinalidad de todas las funciones discontinuas de $\mathbf{R}$ en $\mathbf{R}$ es $2^{2^{\aleph_0}}$. (Sugerencia: use el Ejercicio 2, y muestre que $\left|\mathbf{R}^{\mathbf{R}}\setminus C\right| = 2^{2^{\aleph_0}}$ siempre que $|C| \leq 2^{2^{\aleph_0}}$.)
5. ¿Cuál es la cardinalidad de la familia de conjuntos numerables de números reales?
6. Un subconjunto D de un conjunto ordenado $(A,\leq)$ se llama *denso* si para cualesquiera $x, y \in A$ existe $z \in D$ tal que $x < z < y$. Demuestre que un conjunto ordenado A que tiene un subconjunto denso numerable tiene cardinalidad no mayor que la del continuo.
7. Muestre que la cardinalidad del conjunto de todos los conjuntos abiertos de $\mathbf{R}$ es $2^{\aleph_0}$.

8. Muestre que la cardinalidad del conjunto de todos los conjuntos finitos de $\mathbf{R}$ es $2^{\aleph_0}$.

9. Pruebe que la cardinalidad del conjunto de todas las funciones inyectivas de $\mathbf{N}$ en sí mismo es $2^{\aleph_0}$.

8

El Axioma de Elección

8.1 Introducción

En este capítulo discutiremos un principio que es de los más importantes, y al mismo tiempo controversiales, de las matemáticas. En 1904 Ernst Zermelo en su "*Demostración de que todo conjunto puede ser bien ordenado*" [Z_1] puso atención a una suposición, la cual se usaba implícitamente en una variedad de argumentos matemáticos. Esta suposición no se deduce de los axiomas previamente conocidos de la matemática o de la lógica, por lo tanto, debe ser tomado como un nuevo axioma; Zermelo lo llamó *Axioma de Elección*. El Axioma de Elección es útil porque muchas proposiciones que parece natural suponer verdaderas, no podrían demostrarse sin su ayuda; además, tiene implicaciones significativas en muchas ramas de la matemática, y consecuencias tan poderosas que algunas veces son difíciles de aceptar; pero no siempre es indispensable, puesto que los temas en cuyo contexto se plantean dichas proposiciones continúan subsistiendo también en su ausencia, si bien en forma algo mutilada. La controversia sobre este principio continúa en nuestros días; presentaremos algunos de estos aspectos en este capítulo.

Para ilustrar cuándo el Axioma de Elección se introduce en los argumentos matemáticos examinaremos la siguiente proposición.

Proposición 8.1 *Sea $(A, \leq)$ un conjunto no vacío parcialmente ordenado y supongamos que A no tiene elementos maximales, entonces existe una sucesión creciente $x_0 < x_1 < x_2 < \cdots < x_n < \cdots$ de elementos en A.*

Demostración:

A es no vacío por hipótesis, por lo tanto, podemos seleccionar un elemento arbitrario de A y le llamaremos x_0. Por inducción, supóngase que tenemos dados $x_0 < x_1 < \cdots < x_n$; definamos

$$A_n = \{x \in A : x > x_n\}.$$

A_n es no vacío, pues si fuera vacío, entonces x_n sería un elemento maximal, contradiciendo nuestro supuesto. Seleccionemos un elemento arbitrario de A_n

y llamémosle x_{n+1}; así tenemos

$$x_0 < x_1 < x_2 < \cdots < x_n < x_{n+1}.$$

Este proceso inductivo define una sucesión creciente de longitud n, $S_n = (x_i)_{i=0}^{n-1}$, para cada $n \in \mathbf{N}$. Ahora, si hacemos $S = \bigcup S_n$, entonces S es la sucesión que buscamos. ■

Un examen detallado del argumento anterior nos revelará que hemos usado una suposición que no es en sí misma evidente. En efecto, hemos supuesto que es posible hacer una *sucesión infinita* de elecciones. Es común, en matemáticas, hacer *una* elección arbitraria (por ejemplo, siempre decimos "sea x un elemento arbitrario de A") y la experiencia confirma que podemos hacer una sucesión finita de elecciones; pero una sucesión infinita de elecciones nos lleva a repetir el argumento una cantidad infinita de veces, y nada en nuestra experiencia o en la lógica que habitualmente usamos justifica un proceso de esa naturaleza.

En la prueba de 8.1 fue necesario elegir elementos x_0, x_1, x_2, etc., en sucesión, donde cada elección depende de la elección anterior. El hecho de que las elecciones son sucesivas puede parecer el elemento más molesto en la demostración, puesto que esto involucra un factor de tiempo. Sin embargo, el argumento puede alterarse de tal modo que las elecciones se hagan simultáneamente e independientes unas de otras.

Admitamos que para cada subconjunto no vacío $B \subseteq A$, es posible seleccionar un elemento arbitrario f_B, que podemos llamar el *representante* de B. Note que en este caso, cada elección es independiente de las otras; ya que, en una manera de decirlo, todas las elecciones pueden hacerse simultáneamente. Regresando a la prueba de la Proposición 8.1, si x_n y A_n son dados, podemos definir x_{n+1} como el representante de A_n; en otras palabras, en lugar de seleccionar representantes de A_1, A_2, A_3, etc., en sucesión, tenemos seleccionados representantes de todos los subconjuntos no vacíos de A. De hecho, esto requiere hacer mucho más elecciones de las necesarias para nuestro argumento original, pero es el precio que debemos pagar para substituir las elecciones sucesivas por elecciones simultáneas.

El párrafo precedente hace ver que la naturaleza sucesiva de las elecciones no es el enigma del problema; el cuestionamiento es: ¿*Podemos hacer infinitas elecciones*?

Es fácil observar que en ciertos casos particulares la respuesta es "sí". Por ejemplo, si A es un conjunto bien ordenado, podemos definir el representante de cada subconjunto no vacío $B \subseteq A$ como el elemento mínimo de B. La situación en la Proposición 8.1, sin embargo, es completamente diferente, porque no tenemos alguna regla definida que nos proporcione el representante.

En la demostración de la Proposición 8.1 hablamos de "seleccionar" un elemento de A_n; claramente, es deseable formalizar la noción de *selección* como un nuevo concepto de la Teoría de Conjuntos; la manera de realizarlo es introduciendo el concepto de función selectora de representantes.

Definición 8.2 Sea A un conjunto. Una función *de elección* o *selectora* para A es una función $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ tal que, para todo

$$B \in \mathcal{P}(A) \setminus \{\emptyset\}, \quad f(B) = f_B \in B.$$

Ejemplo 8.3 Sea $A = \{a, b, c\}$. Una función de elección para A es la función dada por la siguiente tabla:

B	f_B
$\{a, b, c\}$	a
$\{a, b\}$	a
$\{a, c\}$	a
$\{b, c\}$	c
$\{a\}$	a
$\{b\}$	b
$\{c\}$	c

De hecho, cualquier conjunto finito tiene una función de elección (ver Ejercicio 8.2.1).

Ejemplo 8.4 Si $(A, \leq)$ es un conjunto bien ordenado entonces A tiene una función de elección.

En vista de la Definición 8.2, podemos reformular la pregunta planteada como: *¿Todo conjunto tiene una función de elección*? Necesitamos hacer un comentario crucial en este punto: la demostración de la Proposición 8.1 no requiere que *construyamos* una función de elección, ésta requiere que exista al menos una función de elección para A, entonces (en el paso controversial de la demostración) definimos $x_{n+1} = f(A_{n+1})$; si estamos seguros de que f existe.

Axioma 9 (de Elección) *Todo conjunto no vacío tiene una función de elección.*

8.2 El Axioma de Elección

El Axioma de Elección difiere de los axiomas **ZF** (axiomas 1 a 8 y 10) por asegurar la existencia de un conjunto (es decir, una función de elección) sin describir a este conjunto como una colección de objetos que tienen una propiedad

particular. Éste es precisamente el aspecto del Axioma de Elección que lo hace inaceptable para un grupo de matemáticos llamados intuicionistas, quienes afirman que la existencia matemática y la constructibilidad son la misma cosa. De hecho, es interesante saber cuándo una proposición matemática puede ser demostrada sin usar el Axioma de Elección.

Por otro lado, K. Gödel [G_2] en 1938 probó que el Axioma de Elección es consistente con los axiomas **ZF**, es decir, no es contradictorio con ellos; tampoco es una consecuencia, como lo demostró P. J. Cohen [C_4] en 1963. Así, este axioma tiene la misma categoría de otros axiomas famosos en matemáticas, como el *Quinto Postulado* de Euclides. Podemos tener entonces una Teoría de Conjuntos "estándar" **ZFC** si aceptamos el Axioma de Elección, y una Teoría de Conjuntos "no estándar" en la cual aceptemos postulados alternativos al Axioma de Elección.

Es imposible, por las razones del párrafo anterior, hacer una decisión en *pro* o en *contra* basada en argumentos de lógica pura acerca de la validez del Axioma de Elección. También, dado que el Axioma de Elección involucra un área de las matemáticas (a saber, los conjuntos infinitos) que está fuera de nuestra experiencia real, nunca será posible confirmar o rechazar al axioma por "observación"; así, la decisión es puramente personal.

En la literatura hay varias formulaciones diferentes del Axioma de Elección las cuales son equivalentes a nuestro Axioma 9. Aquí presentaremos seis de estas proposiciones, otras aparecerán en las siguientes secciones y en los ejercicios.

Teorema 8.5 *Las siguientes proposiciones son equivalentes:*

(a) El Axioma de Elección.

(b) Si $\mathcal{A}$ es una familia no vacía de conjuntos no vacíos y ajenos dos a dos, entonces existe un conjunto B tal que para todo $A \in \mathcal{A}$, $A \cap B$ es un conjunto unitario.

(c) Toda función sobreyectiva tiene una inversa derecha.

(d) Si $\{A_\alpha\}_{\alpha\in\Gamma}$ es tal que $A_\alpha \neq \emptyset$, $A_\alpha \cap A_\beta = \emptyset$ para cualesquiera $\alpha, \beta \in \Gamma$ con $\alpha \neq \beta$, entonces existe $B \subseteq \bigcup_{\alpha\in\Gamma} A_\alpha$ tal que $B \cap A_\alpha$ es unitario para cada $\alpha \in \Gamma$.

(e) Si $\{A_\alpha\}_{\alpha\in\Gamma}$ es una familia indizada de conjuntos no vacíos, entonces existe una función $f : \Gamma \to \bigcup_{\alpha\in\Gamma} A_\alpha$ tal que para cada $\alpha \in \Gamma$, $f(\alpha) \in A_\alpha$.

(f) Si $\{A_\alpha\}_{\alpha\in\Gamma}$ es una familia indizada de conjuntos no vacíos entonces $\prod_{\alpha\in\Gamma} A_\alpha \neq \emptyset$.

(g) Si $F : X \to \mathcal{P}(Y) \setminus \{\emptyset\}$ es una función, entonces existe una función $f : X \to Y$ tal que $f(x) \in F(x)$ para todo $x \in X$.

DEMOSTRACIÓN:

(a) ⇒ (b). Supongamos que $\mathcal{A}$ es una familia no vacía cuyos elementos son no vacíos y ajenos por pares. Sea $A = \bigcup \mathcal{A}$; claramente $\mathcal{A} \subseteq \mathcal{P}(A)$. Por *(a)* existe una función $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ tal que $f(C) \in C$ para cada $C \in \mathcal{P}(A) \setminus \{\emptyset\}$. Si $B = f(\mathcal{A})$, entonces B es el conjunto requerido por *(b)*.

(b) ⇒ (c). Sea $f : X \to Y$ una función sobreyectiva, entonces $A_y = f^{-1}(\{y\}) \neq \emptyset$ para cada $y \in Y$; además $y \neq y'$ implica que $A_y \cap A_{y'} = \emptyset$. Usando *(b)* se infiere la existencia de un conjunto B tal que $B \cap A_y$ es unitario para todo $y \in Y$. Sea $x_y \in X$ tal que $B \cap A_x = \{x_y\}$.

Definamos $g : Y \to X$ tal que $g(y) = x_y \in B \cap A_y$ para cada $y \in Y$. Es inmediato que g está bien definida y que $f(g(y)) = y$; o sea, $f \circ g = Id_Y$.

(c) ⇒ (d). Sea $\mathcal{A} = \{A_\alpha\}_{\alpha\in\Gamma}$ tal que $A_\alpha \neq \emptyset$, $A_\alpha \cap A_\beta = \emptyset$ y definamos $f : \bigcup \mathcal{A} \to A$ como $f(x) = A_\alpha$ si $x \in A_\alpha$. Si $(x, A_\alpha) \in f$ y $(x, A_\beta) \in f$ entonces $A_\alpha \cap A_\beta \neq \emptyset$, luego $A_\alpha = A_\beta$. Por lo tanto, f es una función que claramente es sobreyectiva. Usando la hipótesis existe una función $g : \mathcal{A} \to \bigcup \mathcal{A}$ tal que $f \circ g(A_\alpha) = Id_{\mathcal{A}}(A_\alpha) = A_\alpha$; lo cual implica que $g(A_\alpha) \in A_\alpha$. Tomando $B = g(\mathcal{A})$ se tiene la conclusión.

(d) ⇒ (e). Sea $\{A_\alpha\}_{\alpha\in\Gamma}$ una familia indizada de conjuntos no vacíos. Entonces la familia $\mathcal{A} = \{\{\alpha\} \times A_\alpha\}_{\alpha\in\Gamma}$ cumple las hipótesis requeridas por *(d)*. Por lo tanto, existe un conjunto $B \subseteq \bigcup \mathcal{A}$ tal que $B \cap (\{\alpha\} \times A_\alpha) = \{(\alpha, x_\alpha)\}$ para cada $\alpha \in \Gamma$; sea

$$f = \{(\alpha, x_\alpha) : \alpha \in \Gamma\}.$$

Entonces f es una función de Γ en $\bigcup_{\alpha\in\Gamma} A_\alpha$ y $f(\alpha) = x_\alpha \in A_\alpha$.

(e) ⇒ (f). Sea $\{A_\alpha\}_{\alpha\in\Gamma}$ una familia indizada de conjuntos no vacíos, la función resultante de *(e)* de hecho es un elemento de $\prod_{\alpha\in\Gamma} A_\alpha$.

(f) ⇒ (g). Sea $F : X \to \mathcal{P}(Y) \setminus \{\emptyset\}$ y consideremos $A_x = F(x)$. La hipótesis implica que $\prod_{x\in X} A_x$ es no vacío, es decir, existe

$$f : X \to \bigcup_{x\in X} A_x$$

tal que $f(x) \in A_x = F(x)$. Pero $\bigcup_{x\in X} A_x \subseteq Y$, luego $f : X \to Y$ es la función requerida para establecer *(g)*.

(g) ⇒ (a). Consideremos la función identidad

$$Id : \mathcal{P}(X) \setminus \{\emptyset\} \to \mathcal{P}(X) \setminus \{\emptyset\}.$$

Entonces, por hipótesis, existe $f : \mathcal{P}(X) \setminus \{\emptyset\} \to X$ tal que

$$f(A) \in Id(A) = A;$$

o sea, f es una función de elección para X. ■

Una implicación del Teorema 8.5 es que para cualquier relación de equivalencia en un conjunto X existe un conjunto de representantes para las clases de equivalencia. En los ejercicios se pide mostrar que la unión de una familia numerable de conjuntos numerables es un conjunto numerable; ésta es también una consecuencia del Axioma de Elección. Es importante mostrar que hay otras (muchas) formulaciones equivalentes del Axioma de Elección[1], las cuales tienen aplicación en muy diversas disciplinas matemáticas; en las próximas secciones daremos otras formulaciones, algunas aplicaciones y desventajas que uno sufre al dejar de aceptar el Axioma de Elección. Sierpiński fue uno de los primeros interesados en los problemas relacionados con el Axioma de Elección y desde 1918 publicó numerosos artículos relacionados a este tema.

Ejercicios 8.2

1. Demuestre que cualquier conjunto finito tiene una función de elección.

2. Pruebe que si $(A, \leq)$ es un conjunto linealmente ordenado y si $\mathcal{F}$ es cualquier familia de subconjuntos finitos no vacíos de A, entonces existe una función $f : \mathcal{F} \to A$ tal que $f(F) \in F$ para cada $F \in \mathcal{F}$. (De los axiomas **ZF** no se sigue que cualquier conjunto pueda ser linealmente ordenado.)

3. Pruebe que la unión de una familia numerable de conjuntos numerables es numerable.

4. Pruebe que cualquier conjunto infinito tiene un subconjunto numerable. (Así, con el Axioma de Elección son equivalentes infinito según Dedekind e infinito.)

5. Sea $(A, \leq)$ un conjunto linealmente ordenado no vacío. Muestre que $(A, \leq)$ es bien ordenado si y sólo si no existe una sucesión $(a_n)_{n=0}^{\infty}$ tal que $a_{n+1} < a_n$ para cada $n \in \mathbf{N}$. (Ver Ejercicio 4.5.31.)

[1]Ver por ejemplo [J$_2$] y [RR], donde hay también una extensa bibliografía de trabajos relacionados con los problemas de la independencia lógica del Axioma de Elección y de varias proposiciones más débiles que este axioma.

6. Demuestre las siguientes leyes distributivas.

$$\bigcap_{t\in T}\left(\bigcup_{s\in S} A_{t,s}\right) = \bigcup_{f\in S^T}\left(\bigcap_{t\in T} A_{t,f(t)}\right)$$

$$\bigcup_{t\in T}\left(\bigcap_{s\in S} A_{t,s}\right) = \bigcap_{f\in S^T}\left(\bigcup_{t\in T} A_{t,f(t)}\right).$$

7. Demuestre que el Axioma de Elección es equivalente a la siguiente proposición (Bernays, 1941): Para toda relación R existe una función f tal que $dom\, f = dom\, R$ y $f \subseteq R$.

8. Demuestre que el Axioma de Elección es equivalente a la siguiente proposición (Ward, 1962): El producto cartesiano de una familia de conjuntos no vacíos y mutuamente equipotentes es un conjunto no vacío. (Sugerencia: para una familia $\{X_\alpha\}$ de conjuntos no vacíos, defina $Y = (\bigcup_\alpha X_\alpha)^{\mathbf{N}}$ y $F : Y \times X_\alpha \to Y$ por medio de $F(f,u)(0) = u$ y $F(f,u)(n+1) = f(n)$. Use F para mostrar que $|Y \times X_\alpha| \leq |Y|$; concluya que Y es equipotente a $Y \times X_\alpha$ y emplee la hipótesis.)

8.3 Cuatro Equivalencias Importantes

Hay muchos problemas en Teoría de Conjuntos, Algebra, Análisis y otras ramas de las matemáticas en los cuales el Axioma de Elección o las formas equivalentes que se presentaron en la sección anterior no son inmediatamente aplicables, pero existen otras equivalencias que son muy importantes por sus múltiples aplicaciones. Para demostrarlas necesitamos algunos resultados y definiciones preliminares.

Definición 8.6 Sea $\mathcal{F}$ una familia de conjuntos. Se dice que $\mathcal{F}$ es una *familia de carácter finito* si para cada conjunto A, se tiene que $A \in \mathcal{F}$ si y sólo si cada subconjunto finito de A pertenece a $\mathcal{F}$.

Lema 8.7 *Sea $\mathcal{F}$ una familia de carácter finito y sea $\mathcal{B}$ una cadena en $\mathcal{F}$ con respecto a la contención, entonces $\bigcup \mathcal{B} \in \mathcal{F}$.*

Demostración:

Es suficiente mostrar que cada subconjunto finito de $\bigcup \mathcal{B}$ pertenece a $\mathcal{F}$. Sea $F = \{x_1, x_2, \ldots, x_n\} \subseteq \bigcup \mathcal{B}$. Entonces, existen $B_i \in \mathcal{B}$ para $i \in \{1, 2, \ldots, n\}$ tal que $x_i \in B_i$. Como $\mathcal{B}$ es una $\subseteq$-cadena, existe $i_0 \in \{1, 2, \ldots, n\}$ tal que

$B_i \subseteq B_{i_0}$ para cada $i \in \{1, 2, \ldots, n\}$. Entonces $F \subseteq B_{i_0} \in \mathcal{F}$, pero $\mathcal{F}$ es de carácter finito, así que $F \in \mathcal{F}$. Por lo tanto, $\bigcup \mathcal{B} \in \mathcal{F}$. ■

Teorema 8.8 (Lema de Tukey-Teichmüller) *Toda familia no vacía de - carácter finito tiene un elemento $\subseteq$-maximal.*

Demostración:

Supongamos que el resultado es falso, entonces existe una familia no vacía $\mathcal{F}$ de carácter finito que no tiene elementos maximales. Para cada $F \in \mathcal{F}$, sea

$$\mathcal{A}_F = \{E \in \mathcal{F} : F \subset E\}.$$

Entonces $\{\mathcal{A}_F : F \in \mathcal{F}\}$ es una familia no vacía de conjuntos no vacíos. Por el Teorema 8.5(e), existe una función f definida en $\mathcal{F}$ tal que $f(F) \in \mathcal{A}_F$ para cada $F \in \mathcal{F}$. Así tenemos que $F \subset f(F) \in \mathcal{F}$ para todo $F \in \mathcal{F}$.

Una subfamilia $\mathcal{J}$ de $\mathcal{F}$ se llama *f-inductiva* si tiene las siguientes propiedades:

(1) $\emptyset \in \mathcal{J}$;

(2) $A \in \mathcal{J}$ implica $f(A) \in \mathcal{J}$;

(3) si $\mathcal{B}$ es una $\subseteq$-cadena contenida en $\mathcal{J}$, entonces $\bigcup \mathcal{B} \in \mathcal{J}$.

Ya que $\emptyset$ es un conjunto finito, $\emptyset \in \mathcal{F}$, y por el Lema 8.7, la familia $\mathcal{F}$ es f-inductiva. Así, el sistema de subfamilias de $\mathcal{F}$ que son f-inductivas es no vacío. Sea

$$\mathcal{J}_0 = \bigcap \{\mathcal{J} \subseteq \mathcal{F} : \mathcal{J} \text{ es } f\text{-inductiva}\}.$$

Es fácil ver que $\mathcal{J}_0$ es f-inductiva. Así, $\mathcal{J}_0$ es la mínima familia f-inductiva, es decir, cualquier familia f-inductiva contenida en $\mathcal{J}_0$, debe ser $\mathcal{J}_0$. Emplearemos fuertemente este hecho para mostrar que $\mathcal{J}_0$ es una cadena.

Sea

$$\mathcal{H} = \{A \in \mathcal{J}_0 : B \in \mathcal{J}_0 \text{ y } B \subset A \text{ implica } f(B) \subseteq A\}.$$

Se afirma que si $A \in \mathcal{H}$ y $C \in \mathcal{J}_0$, entonces o bien $C \subseteq A$ o $f(A) \subseteq C$. Para probar esta afirmación, sea $A \in \mathcal{H}$ y definamos

$$\mathcal{G}_A = \{C \in \mathcal{J}_0 : C \subseteq A \ \vee \ f(A) \subseteq C\}.$$

Será suficiente mostrar que $\mathcal{G}_A$ es f-inductiva.

Como $\emptyset \in \mathcal{J}_0$ y $\emptyset \subseteq A$, (1) se satisface. Sea $C \in \mathcal{G}_A$, entonces o bien $C \subset A$, $C = A$ o $f(A) \subseteq C$. Si $C \subset A$, entonces $f(C) \subseteq A$ puesto que $A \in \mathcal{H}$. Si $C = A$, entonces $f(A) \subseteq f(C)$. Si $f(A) \subseteq C$, entonces $f(A) \subseteq f(C)$ puesto

que $C \subset f(C)$. Así, en cualquier caso $f(C) \in \mathcal{G}_A$ y (2) se satisface. Sea $\mathcal{B}$ una cadena en $\mathcal{G}_A$. Entonces, o bien $C \subseteq A$ para cada $C \in \mathcal{B}$, y en tal caso $\bigcup \mathcal{B} \subseteq A$; o existe $C \in \mathcal{B}$ tal que $f(A) \subseteq C \subseteq \bigcup \mathcal{B}$. Así $\bigcup \mathcal{B} \in \mathcal{G}_A$ y (3) se satisface. Concluimos que $\mathcal{G}_A$ es f-inductiva y así $\mathcal{G}_A = \mathcal{J}_0$.

Ahora afirmamos que $\mathcal{H} = \mathcal{J}_0$. Para probar esto, mostraremos que $\mathcal{H}$ es f-inductiva. Como $\emptyset$ no tiene subconjuntos propios, $\mathcal{H}$ satisface (1) por vacuidad. Supongamos ahora que $A \in \mathcal{H}$ y $B \in \mathcal{J}_0$ es tal que $B \subset f(A)$. Como $B \in \mathcal{J}_0 = \mathcal{G}_A$ y dado que la inclusión $f(A) \subseteq B$ es imposible, tenemos que $B \subseteq A$. Si $B \subset A$, entonces, por la definición de $\mathcal{H}$, $f(B) \subseteq A \subset f(A)$. Si $B = A$, entonces $f(B) \subseteq f(A)$. En cualquier caso se obtiene que $f(B) \subseteq f(A)$; así $f(A) \in \mathcal{H}$ y (2) se satisface para $\mathcal{H}$. Finalmente, sea $\mathcal{B}$ una cadena en $\mathcal{H}$ y sea $B \in \mathcal{J}_0$ tal que $B \subset \bigcup \mathcal{B}$. Veamos que $f(B) \subseteq \bigcup \mathcal{B}$. Como $B \in \mathcal{J}_0 = \mathcal{G}_A$ para cada $A \in \mathcal{B}$, tenemos que, o bien $B \subseteq A$ para algún $A \in \mathcal{B}$, o $f(A) \subseteq B$ para cada $A \in \mathcal{B}$. Si la última alternativa fuera cierta, tendríamos que

$$B \subset \bigcup \mathcal{B} \subseteq \bigcup \{f(A) : A \in \mathcal{B}\} \subseteq B,$$

lo cual es imposible. Así, existe algún $A \in \mathcal{B}$ tal que $B \subseteq A$. Si $B \subset A$, entonces como $A \in \mathcal{H}$, tenemos que $f(B) \subseteq A \subseteq \bigcup \mathcal{B}$. Si $B = A$, entonces $B \in \mathcal{H}$ y $\bigcup \mathcal{B} \in \mathcal{J}_0 = \mathcal{G}_B$. Esto implica que $f(B) \subseteq \bigcup \mathcal{B}$ ($\bigcup \mathcal{B} \subseteq B$ es imposible). Así en cualquier caso, $f(B) \subseteq \bigcup \mathcal{B}$ y, por tanto, $\bigcup \mathcal{B} \in \mathcal{H}$. Esto muestra que $\mathcal{H}$ satisface (3). Por todo lo anterior concluimos que $\mathcal{H}$ es f-inductiva y $\mathcal{H} = \mathcal{J}_0$.

De los argumentos anteriores podemos inferir que si $A \in \mathcal{J}_0 = \mathcal{H}$ y $B \in \mathcal{J}_0 = \mathcal{G}_A$, entonces o bien $B \subseteq A$ o $A \subseteq f(A) \subseteq B$, es decir, cualesquiera dos elementos de $\mathcal{J}_0$ son $\subseteq$-comparables; con lo cual $\mathcal{J}_0$ es una cadena. Sea $M = \bigcup \mathcal{J}_0$. Puesto que $\mathcal{J}_0$ es f-inductiva, (3) implica que $M \in \mathcal{J}_0$. Aplicando (2) tenemos que

$$\bigcup \mathcal{J}_0 = M \subset f(M) \in \mathcal{J}_0.$$

Esta contradicción establece el teorema. ■

Teorema 8.9 (Principio Maximal de Hausdorff) *Todo conjunto no vacío (parcialmente) ordenado contiene una cadena $\subseteq$-maximal.*

Demostración:

Sea $(X, \leq)$ cualquier conjunto ordenado no vacío. Queremos mostrar que X contiene una cadena $\subseteq$-maximal. Esto se implica fácilmente del Lema de Tukey-Teichmüller puesto que la familia $\mathcal{C}$ de todas las cadenas en X es no vacía y de carácter finito. ■

Teorema 8.10 (Lema de Kuratowski-Zorn) *Cualquier conjunto (parcialmente) ordenado y no vacío en el cual toda cadena tiene una cota superior tiene un elemento maximal.*

DEMOSTRACIÓN:

Sea $(X, \leq)$ cualquier conjunto ordenado no vacío en el cual cada cadena tiene una cota superior. Usando el Principio Maximal de Hausdorff existe una cadena $\subseteq$-maximal $M \subseteq X$. Sea m una cota superior de M. Entonces m es un elemento maximal de X, pues si existe algún $x \in X$ tal que $m < x$, entonces $M \cup \{x\}$ es una cadena que contiene propiamente a M. Esto contradice la maximalidad de M. ■

El cuarto resultado importante que presentamos en esta sección, es una de las consecuencias más importantes del Axioma de Elección y es un ejemplo fuera de lo común de una proposición que no es constructiva. Ésta asegura que cualquier conjunto puede ser bien ordenado. Su demostración no proporciona información alguna de cómo bien ordenar a los elementos de X; en otras palabras, *no* asegura que cualquier conjunto pueda ser *efectivamente* bien ordenado sino que se limita a asegurar que, entre todas las posibles relaciones $R \subseteq X \times X$ hay al menos una que es un buen orden para X.

Un conjunto finito X puede ser obviamente bien ordenado; por ejemplo, si $X = \{a, b, c\}$, entonces $a < b < c$ es un buen orden de X. Sin embargo, no ha sido descubierto algún método para bien ordenar conjuntos tales como $\mathbf{R}$, el conjunto de los números reales. En efecto, según la opinión de muchos matemáticos, es imposible construir un buen orden para $\mathbf{R}$.

Ahora probaremos el Teorema del Buen Orden; note que la demostración está basada fuertemente en el Axioma de Elección.

Sea X un conjunto arbitrario, y sea $\mathcal{B}$ la familia de todos los pares (B, G) donde B es un subconjunto de X y G es un buen orden para B. Introducimos el símbolo $\preceq$ y definimos $(B, G) \preceq (B', G')$ si y sólo si

$$B \subseteq B', \qquad G \subseteq G', \qquad x \in B,\, y \in B' \setminus B \Rightarrow (x, y) \in G'$$

(Note que la última condición asegura, intuitivamente, que todos los elementos de B preceden a todos los elementos de $B' \setminus B$.)

A (B', G') se le llama *continuación* de (B, G). Es fácil verificar que $\preceq$ es una relación de orden en $\mathcal{B}$; los detalles se dejan como ejercicio al lector.

Lema 8.11 *Sean $(\mathcal{B}, \preceq)$ el conjunto ordenado antes definido,*

$$\mathcal{C} = \{(B_\alpha, G_\alpha)\}_{\alpha \in I}$$

una cadena en $\mathcal{B}$ *y*

$$B = \bigcup_{\alpha \in I} B_\alpha \quad , \quad G = \bigcup_{\alpha \in I} G_\alpha.$$

Entonces $(B, G) \in \mathcal{B}$.

Demostración:

Claramente $B \subseteq X$; así nuestro resultado será establecido si podemos mostrar que G es un buen orden para B. Primero verifiquemos que G es una relación de orden.

Reflexividad. $x \in B$ implica $x \in B_\alpha$ para algún $\alpha \in I$, entonces $(x, x) \in G_\alpha \subseteq G$; así G es reflexiva.

Antisimetría. Si $(x, y) \in G$ y $(y, x) \in G$, entonces $(x, y) \in G_\alpha$ y $(y, x) \in G_\beta$ para algunos $\alpha, \beta \in I$; pero como $\mathcal{C}$ es una cadena en $\mathcal{B}$, $G_\alpha \subseteq G_\beta$ o $G_\beta \subseteq G_\alpha$. Supongamos que $G_\alpha \subseteq G_\beta$. Entonces $(x, y) \in G_\beta$ y $(y, x) \in G_\beta$, pero G_β es una relación de orden, así $x = y$. Esto prueba que G es antisimétrica.

Transitividad. Si $(x, y) \in G$ y $(y, z) \in G$, entonces existen $\alpha, \beta \in I$ tales que $(x, y) \in G_\alpha$ y $(y, x) \in G_\beta$; nuevamente usando que $\mathcal{C}$ es una cadena, podemos suponer, sin pérdida de generalidad, que $G_\alpha \subseteq G_\beta$. Entonces $(x, y) \in G_\beta$ y $(y, z) \in G_\beta$ implica $(x, z) \in G_\beta \subseteq G$, lo cual muestra que G es transitiva.

Ahora demostraremos que B está bien ordenado por G. Sea $D \subseteq B,\ D \neq \emptyset$. Entonces $D \cap B_{\alpha_0} \neq \emptyset$ para algún $\alpha_0 \in I$; luego $D \cap B_{\alpha_0} \subseteq B_{\alpha_0}$. Por lo tanto, $D \cap B_{\alpha_0}$ tiene un primer elemento b en el orden G_{α_0}; esto es, para todo $y \in D \cap B_{\alpha_0}$, $(b, y) \in G_{\alpha_0}$. Procedamos a demostrar que b es el primer elemento de D en (B, G).

Sea $x \in D$. Si $x \in B_{\alpha_0}$, entonces $(b, x) \in G_{\alpha_0} \subseteq G$. Si por el contrario $x \notin B_{\alpha_0}$ entonces, puesto que $x \in D \subseteq B$, necesariamente $x \in B_\beta$ para algún $\beta \in I$. Ahora como $B_\beta \nsubseteq B_{\alpha_0}$, no puede ocurrir que $(B_\beta, G_\beta) \preceq (B_{\alpha_0}, G_{\alpha_0})$. Pero $\mathcal{C}$ es una cadena, entonces forzosamente $(B_{\alpha_0}, G_{\alpha_0}) \preceq (B_\beta, G_\beta)$. Por la definición de $\preceq$, $(b, x) \in G_\beta \subseteq G$. Esto demuestra que $b = \min D$ en (B, G). ■

Lema 8.12 *Si* $\mathcal{C}$, B *y* G *están definidos como antes,* (B, G) *es una cota superior de* $\mathcal{C}$ *en* $(\mathcal{B}, \preceq)$.

Demostración:

Sea $(B_\alpha, G_\alpha) \in \mathcal{C}$; claramente $B_\alpha \subseteq B$ y $G_\alpha \subseteq G$. Ahora supóngase que $x \in B_\alpha$, $y \in B \setminus B_\alpha$; ciertamente $y \in B_\beta$ para algún $\beta \in I$. Ahora $(B_\alpha, G_\alpha) \preceq (B_\beta, G_\beta)$ pues $y \in B_\beta \setminus B_\alpha$, de aquí resulta que $(x, y) \in G_\beta \subseteq G$. Esto es, $(B_\alpha, G_\alpha) \preceq (B, G)$. ■

Teorema 8.13 (del Buen Orden) *Todo conjunto puede ser bien ordenado.*

DEMOSTRACIÓN:

Por los Lemas 8.11 y 8.12 podemos aplicar el Lema de Kuratowski-Zorn a $(\mathcal{B}, \preceq)$; así $\mathcal{B}$ tiene un elemento $\preceq$-maximal (B, G). Mostraremos que $B = X$, así X será bien ordenado. Si $B \subset X$, entonces existe $x \in X \setminus B$. Adjuntando x como último elemento de B (ver Ejemplo 4.132), tenemos que

$$(B, G) \prec (B \cup \{x\}, G \cup \{(a, x) : a \in B\}).$$

Esto contradice el carácter maximal de (B, G). Por lo tanto, $B = X$. ■

Es claro que el Axioma de Elección puede derivarse del Teorema del Buen Orden. En efecto, si X es un conjunto no vacío, por el Teorema del Buen Orden, X puede ser bien ordenado; si B es un subconjunto no vacío de X, sea $f(B) = \min B$. Entonces f es una función de elección.

Tenemos pues probado el siguiente teorema que resalta los resultados que presentamos en esta sección.

Teorema 8.14 *Son equivalentes:*

(a) El Axioma de Elección.
(b) El Lema Tukey-Teichmüller.
(c) Principio Maximal de Hausdorff.
(d) El Lema de Kuratowski-Zorn.
(e) El Teorema del Buen Orden.

El Teorema del Buen Orden fue propuesto originalmente por Cantor, y aunque él no dio alguna demostración, D. Hilbert en el Congreso Internacional de Matemáticas en París (1900) se refirió al Teorema del Buen Orden como un resultado de Cantor. Zermelo fue el primero en demostrarlo; sin embargo, debido a la paradoja de Burali-Forti y a que su demostración hacía uso de inducción transfinita, esa primera demostración de Zermelo no fue muy aceptada. Para responder a las críticas, en 1908 Zermelo publicó otra demostración en la que se eliminaba el uso de ordinales. Se dice que la forma axiomática de Zermelo para la Teoría de Conjuntos está fuertemente influenciada por la segunda demostración ya que, hablando vagamente, él seleccionó las formas más débiles para los axiomas en los cuales pudiera justificar su demostración.

La segunda formulación del Axioma de Elección la realizó B. Russell bajo el nombre de Axioma Multiplicativo (1906). Aunque Russell anunció que su principio era un sustituto del principio de Zermelo (creía que era más débil que el principio de Zermelo). Después, en 1909, F. Hausdorff propuso el Principio Maximal; sin embargo, Hausdorff no lo menciona en su famoso libro

Mengenlehre de 1914 y aparece hasta la segunda edición de 1927. Kuratowski redescubrió el Principio Maximal en 1922 y dio otra demostración del Teorema del Buen Orden. El segundo redescubrimiento lo realizó Zorn en 1935, en esta ocasión el Principio Maximal fue decisivamente convincente, el resultado se conoce como el "Lema de Zorn". Similarmente Teichmüller en 1939 y Tukey 1940 formularon independientemente el otro principio maximal.

Ejercicios 8.3

1. Muestre que la intersección de un sistema de familias f-inductivas es una familia f-inductiva.

2. Muestre que la relación $\preceq$ (continuación) definida antes del Lema 8.11 es un orden parcial.

3. Demuestre que si A puede ser bien ordenado, entonces $\mathcal{P}(A)$ puede ser linealmente ordenado. (Sugerencia: considere el primer elemento de $X \triangle Y$, para $X, Y \subseteq A$.)

4. Sea $(A, \leq)$ un conjunto parcialmente ordenado en el que cualquier cadena tiene una cota superior. Muestre que para cada $a \in A$, existe un elemento $\leq$-maximal $x \in A$ tal que $a \leq x$.

5. Sea $(L, \leq)$ un conjunto linealmente ordenado. Pruebe que existe un conjunto $W \subseteq L$ tal que $\leq$ es un buen orden en W y tal que para cada $x \in L$ existe un $y \in W$ tal que $x \leq y$.

6. Sea A cualquier conjunto infinito. Demuestre que A puede ser bien ordenado de tal manera que A no tenga máximo. También muestre que hay un buen orden para A en el cual A tiene máximo.

7. Pruebe que si $\mathcal{A}$ es una familia de carácter finito, entonces cualquier $X \in \mathcal{A}$ está incluido en un $\subseteq$-maximal $Y \in \mathcal{A}$.

8. Demuestre que la siguiente proposición es equivalente al Axioma de Elección: Cualquier familia $\mathcal{F}$ contiene una subfamilia $\subseteq$-maximal consistente de conjuntos ajenos por pares. (Sugerencia: sea $\mathcal{S}$ una familia de conjuntos ajenos; encuentre una función de elección para $\mathcal{S}$. Esto puede obtenerse usando una subfamilia $\subseteq$-maximal de conjuntos ajenos de

$$\mathcal{E} = \{\{(0, a), (1, A)\} : A \in \mathcal{S} \text{ y } a \in A\}.)$$

9. Pruebe que el Principio Maximal de Hausdorff es equivalente a la siguiente proposición: Si $\mathcal{A}$ es una familia tal que para cada cadena $\mathcal{B} \subseteq \mathcal{A}$, $\bigcup \mathcal{B} \in \mathcal{A}$, entonces $\mathcal{A}$ tiene un elemento $\subseteq$-maximal.

10. Demuestre que para cualquier orden $\preceq$ en A, existe un orden lineal $\leq$ en A tal que $a \preceq b$ implica $a \leq b$ para todo $a, b \in A$ (es decir, cualquier orden parcial puede extenderse a un orden lineal.) (Sugerencia: sea $\mathcal{O}$ la familia de ordenes de A que contienen a $\leq$. Use el ejercicio anterior para mostrar que $\mathcal{O}$ tiene un elemento $\subseteq$-maximal, $\preceq$. Si ocurriera que $a \not\preceq b$ y $b \not\preceq a$ para algunos $a, b \in A$, considere la relación

$$\preceq \cup \{(x, y) : x \preceq a \text{ y } b \preceq y\}.)$$

8.4 Uso del Axioma de Elección

Empezamos con algunos resultados ampliamente conocidos en los cuales pocas veces se enfatiza el uso del Axioma de Elección.

Un número real x está en la clausura $\overline{A}$, de un conjunto $A \subseteq \mathbf{R}$, si para cualquier $\epsilon > 0$,

$$A \cap (x - \epsilon, x + \epsilon) \neq \emptyset.$$

En el siguiente ejemplo se proporciona una caracterización de los puntos clausura.

Ejemplo 8.15 Un número real x está en la clausura de un conjunto $A \subseteq \mathbf{R}$ si y sólo si existe una sucesión de elementos en A que converge a x.

Demostración:

$\Rightarrow$] Si $x \in \overline{A}$, entonces para cada $n \in \mathbf{N}$ podemos seleccionar $x_n \in A \cap (x - \frac{1}{n}, x + \frac{1}{n})$; como $|x - x_n| < \frac{1}{n}$ para cada $n \in \mathbf{N}$, se sigue fácilmente que $\lim_{n\to\infty} x_n = x$.

$\Leftarrow$] Está parte de la demostración no hace uso del Axioma de Elección y es fácil. ■

Cuando se demuestra en los cursos ordinarios de Cálculo Diferencial e Integral o Análisis la proposición del Ejemplo 8.15 se pone mucha atención a la convergencia de la sucesión y se deja de lado la elección de sus términos, siendo que, en realidad, es más importante la elección, pues de ella se deduce la convergencia.

Otro ejemplo similar es la equivalencia entre la definición ϵ-δ de continuidad y la definición de continuidad secuencial.

Ejemplo 8.16 Una función $f : (a, b) \to \mathbf{R}$ es continua en un punto $x \in (a, b)$ si y sólo si para cada sucesión $\{x_n\}_{n\in\mathbf{N}}$ de elementos en (a, b) tal que $\lim x_n = x$ se tiene que $\lim f(x_n) = f(x)$.

Demostración:

Demostraremos únicamente la parte que hace uso del Axioma de Elección, es decir, la suficiencia. Si f es discontinua en $x \in (a, b)$, entonces existe un $\epsilon > 0$ tal que para cada $n \in \mathbf{N}$, existe $x_n \in (a, b) \cap (x - \frac{1}{n}, x + \frac{1}{n})$ tal que $|f(x) - f(x_n)| \geq \epsilon$. Entonces $\lim_{n\to\infty} x_n = x$, pero es falso que

$$\lim_{n\to\infty} f(x_n) = f(x). \blacksquare$$

La compacidad es una de las propiedades topológicas más importantes. La equivalencia entre compacidad y compacidad secuencial en $\mathbf{R}$ también hace uso del Axioma de Elección.

Ejemplo 8.17 Un conjunto $K \subseteq \mathbf{R}$ es compacto si y sólo si toda sucesión de elementos en K tiene una subsucesión convergente.

Otras consecuencias ya más especiales son las siguientes. Posiblemente, la más famosa de estas consecuencias se debe a Vitali [V] en 1905.

Ejemplo 8.18 Existen subconjuntos de $\mathbf{R}$ no medibles según Lebesgue.

Demostración:

Sea μ la medida de Lebesgue en $\mathbf{R}$. Es conocido que μ es numerablemente aditiva, invariante por traslación y que $\mu([a, b]) = b-a$ para cualquier intervalo $[a, b]$.

Sea Z un conjunto de representantes de las clases de equivalencia módulo $\equiv$ en $[0, 1]$ dada por $x \equiv y$ si y sólo si $y - x \in \mathbf{Q}$. Utilizando los resultados y la notación del Ejercicio 4.4.16,

$$\mu([0, 1]) = \mu\left(\bigcup_{r\in Q} Z(r)\right) = \sum_{r\in\mathbf{Q}} \mu(Z(r)).$$

Como $\mu([0, 1]) = 1$, $\mu(Z(r_0)) \neq 0$ al menos para algún $r_0 \in \mathbf{Q}$. Pero $\mu(Z(r_0)) = \mu(Z(r))$ para cada $r \in \mathbf{Q}$ ya que μ es invariante por traslaciones; con lo cual $\mu([0, 1]) = \infty$, que es imposible. Por lo tanto, Z no es medible según Lebesgue. $\blacksquare$

Sea L una retícula (ver Ejercicio 4.5.20), un ideal en L es un subconjunto propio no vacío I de L tal que

(i) $a \in I$ y $b \leq a$ implica $b \in I$;
(ii) $a \in I$ y $b \in I$ implica $a \perp b := \inf\{a, b\} \in I$.

Una retícula se llama *unitaria* si existe un elemento $1 \in L$ tal que $1 \perp a = a$ para cada $a \in L$.

Ejemplo 8.19 Cualquier retícula unitaria tiene un ideal maximal.

DEMOSTRACIÓN:

Sea $\mathcal{F}$ la familia de todos los ideales en la retícula dada. La familia $\mathcal{F}$ satisface las hipótesis del Lema de Kuratowski-Zorn y así tiene un elemento maximal. ■

Ejemplo 8.20 (Bases de Hamel) Todo espacio vectorial tiene una base.

DEMOSTRACIÓN:

Sea $\mathcal{F}$ la familia de todos los subconjuntos de vectores linealmente independientes. Obviamente, la familia $\mathcal{F}$ tiene carácter finito y así por el Lema de Tukey-Teichmüller, existe un conjunto $\subseteq$-maximal linealmente independiente ß. Usando la maximalidad, se prueba sin dificultad que ß es una base. ■

Andreas Blass en 1984 demostró que la proposición del Ejemplo 8.20 implica el Axioma de Elección.

Un grupo G es un *grupo libre* si tiene un conjunto de generadores A con la siguiente propiedad: Todo elemento g de G distinto del neutro 1 puede ser *unívocamente* escrito en la forma

$$a_1^{\pm 1} a_2^{\pm 1} \cdots a_n^{\pm 1},$$

donde los $a_i \in A$ y a no aparece adyacente a a^{-1} para cualquier $a \in A$.

Ejemplo 8.21 (Teorema de Nielson-Schreir) Todo subgrupo de un grupo libre es un grupo libre.

La demostración de este teorema es difícil y queda fuera de nuestro alcance. Únicamente mencionaremos que usa el hecho de que el subgrupo dado puede ser bien ordenado y esto se usa para construir, por inducción transfinita, un conjunto de generadores libres del subgrupo.

Una *clausura algebraica* de un campo F es una extensión C algebraicamente cerrada sobre F, es decir, un campo C en el cual todo polinomio no constante tiene una raíz y cualquier elemento de C es raíz de un polinomio con coeficientes en F. El artículo de Zorn [Z_3], donde introduce su principio maximal, se dedica a demostrar el siguiente teorema.

Ejemplo 8.22 (Clausura Algebraica) Todo campo tiene una única (salvo isomorfismo) clausura algebraica.

El siguiente es otro resultado equivalente al Axioma de Elección; fue establecido por G. Klimovski en 1962 y U. Felgner en 1976.

Ejemplo 8.23 Todo grupo contiene un subgrupo abeliano $\subseteq$-maximal.

Sea E un espacio vectorial real. Un funcional lineal sobre E es una función $\varphi : E \to \mathbf{R}$ tal que

$$\varphi(rx + sy) = r\varphi(x) + s\varphi(y)$$

para todo $x, y \in E$ y $r, s \in \mathbf{R}$. Una función $p : E \to \mathbf{R}$ es un funcional sublineal si

$$p(x + y) \leq p(x) + p(y)$$

para todo $x, y \in E$ y

$$p(ry) = rp(x)$$

para todo $x \in E$, $r \geq 0$.

Ejemplo 8.24 (Teorema de Hahn-Banach) Sea p un funcional sublineal sobre un $\mathbf{R}$-espacio vectorial E y sea φ un funcional lineal sobre un subespacio vectorial V de E tal que $\varphi(x) \leq p(x)$ para todo $x \in V$. Entonces existe un funcional Φ definido sobre E el cual extiende a φ y $\Phi(x) \leq p(x)$ para todo $x \in E$.

Demostración:

Considérese la familia $\mathcal{F}$ de todos los funcionales ψ definidos sobre un subespacio de E, que extienden a φ y que satisfacen $\psi(x) \leq p(x)$ para todo $x \in dom\,\psi$. Definamos $\leq$ en $\mathcal{F}$ como $\psi \leq \psi'$ si y sólo si $\psi \subseteq \psi'$. Entonces $(\mathcal{F}, \leq)$ es un conjunto parcialmente ordenado. Sea $\mathcal{C}$ una cadena en $\mathcal{F}$. Es fácil verificar que $\mathcal{C}$ es un sistema compatible de funciones. Entonces

$$W = \bigcup \{dom\,\psi : \psi \in \mathcal{F}\}$$

es un subespacio vectorial de E y $\Psi = \bigcup \mathcal{C}$ es un funcional lineal sobre W. Más aún, si $x \in W$, $\Psi(x) = \psi(x)$ para algún $\psi \in \mathcal{C}$, y así $\Psi(x) \leq p(x)$. Aplicando el Lema de Kuratowski-Zorn vemos que $\mathcal{F}$ tiene un elemento maximal, digamos Φ. Para completar la demostración se necesita demostrar que $dom\,\Phi = E$. Esta parte de la demostración no utiliza el Axioma de Elección y, por su extensión, la omitiremos. ■

Por sus bastas consecuencias, el Teorema de Hahn-Banach es de los más importantes en el Análisis Funcional. En 1970 P. R. Andenaes estableció la siguiente versión más fuerte del Teorema de Hahn-Banach y J. Lembcke en 1974 demostró que el resultado de Andenaes implica el Axioma de Elección.

Ejemplo 8.25 Sea X un $\mathbf{R}$-espacio vectorial, Y un subespacio vectorial de X y S un subconjunto de X. Supóngase que $p : X \to R$ es un funcional sublineal sobre X y $f : Y \to R$ un funcional lineal tal que $f(y) \leq p(y)$. Entonces el conjunto $\mathcal{Z}$ de todas las extensiones lineales p-dominadas de f a X tiene un elemento g tal que, para todo $h \in \mathcal{Z}$ que cumple $g(s) \leq h(s)$ para cada $s \in S$, se tiene que $g = h$ en S. Esto es, g es S-maximal en $\mathcal{Z}$.

En el siguiente ejemplo veremos un conocido resultado del Análisis Funcional que implica el Axioma de Elección, según demostraron L. J. Bell y Fremlin en 1972.

Por un *punto extremo* de un conjunto convexo K de un espacio vectorial se entiende un punto que no es interior a cualquier segmento contenido en K.

Ejemplo 8.26 La esfera unitaria en el dual de un $\mathbf{R}$-espacio vectorial normado tiene un punto extremo.

Sea $\{(X_\alpha, \tau_\alpha)\}_{\alpha\in\Gamma}$ una familia de espacios topológicos. El producto topológico de la familia $\{(X_\alpha, \tau_\alpha)\}_{\alpha\in\Gamma}$ es definida como el producto cartesiano

$$X = \prod_{\alpha\in\Gamma} X_\alpha$$

de la familia $\{X_\alpha\}_{\alpha\in\Gamma}$ equipado con la topología más débil que hace a las proyecciones continuas.

Ejemplo 8.27 (Teorema de Tychonoff) El producto topológico de espacios compactos es compacto.

Una demostración, más o menos popular, de este teorema usa la caracterización de la compacidad por filtros.

Un *filtro* $\mathcal{F}$ sobre un conjunto X es un subconjunto propio no vacío del conjunto potencia de X tal que:

$A \in \mathcal{F}$ y $A \subseteq B$ implica $B \in \mathcal{F}$;
$A \in \mathcal{F}$ y $B \in \mathcal{F}$ implica $A \cap B \in \mathcal{F}$.

Un *ultrafiltro* $\mathcal{F}$ sobre X, es un filtro sobre X tal que para cada $A \subseteq X$, o bien $A \in \mathcal{F}$ o $X \setminus A \in \mathcal{F}$. Una familia $\mathcal{B}$ es *base de filtro* si la familia de subconjuntos de X que contienen a intersecciones finitas de elementos de $\mathcal{B}$,

$$\{A \in \mathcal{P}(X) : A \supseteq A_1 \cap A_2 \cap \cdots \cap A_k, \quad A_1, A_2, \ldots, A_k \in \mathcal{B}\},$$

es un filtro sobre X.

Un espacio X es compacto si y sólo si para cada base de filtro $\mathcal{B}$ sobre X,

$$\bigcap \{\overline{A} : A \in \mathcal{B}\} \tag{8.4.1}$$

es no vacía.

Sea $(X, \tau) = \prod_{\alpha\in\Gamma}(X_\alpha, \tau_\alpha)$ un producto de espacios compactos. La familia de todas las bases de filtros sobre X tiene carácter finito y así por el Lema de Tukey-Teichmüller, toda base de filtro está incluida en una base de filtro maximal (un ultrafiltro). Para mostrar que la intersección (8.4.1) es no vacía siempre que $\mathcal{B}$ sea maximal (lo cual es obviamente suficiente), haremos lo siguiente:

(1) la compacidad de los espacios (X_α, τ_α) implica que las intersecciones de las proyecciones $A_\alpha = \bigcap \left\{\overline{p_\alpha(B)} : B \in \mathcal{B}\right\}$ es no vacía;

(2) con el Axioma de Elección nuevamente, tomemos $x_\alpha \in A_\alpha$ para cada α, y

(3) la maximalidad de $\mathcal{B}$ implica que el punto $x = (x_\alpha)_{\alpha\in\Gamma}$ pertenece a la intersección $\bigcap \{\overline{A} : A \in \mathcal{B}\}$.

Por lo tanto, el espacio (X, τ) es compacto.

En 1935 S. Kakutani conjeturó que el Axioma de Elección es una consecuencia del Teorema de Tychonoff. Quince años después J. L. Kelley publicó su famoso artículo donde mostraba que el Teorema de Tychonoff implica el Axioma de Elección [K_2]; sin embargo, J. D. Halpern en [H_3] mostró que la demostración de Kelley es deficiente. J. Łos y C. Ryll-Nardzewski observaron que la demostración de Kelley muestra que el Teorema de Tychonoff para espacios compactos de Hausdorff implica el Axioma de Elección para espacios compactos de Hausdorff no vacíos. Pese a todas estas observaciones, la demostración de Kelley es esencialmente correcta. L. E. Ward en 1962 mostró que una versión más débil del Teorema de Tychonoff es equivalente al Axioma de Elección. Posteriormente O. T. Alas en 1969 probó que una versión aún más débil era también equivalente al Axioma de Elección:

Proposición 8.28 *Son equivalentes:*

(a) El Axioma de Elección.

(b) El Teorema de Tychonoff.

(c) El producto topológico de una familia de espacios topológicos compactos, mutuamente homeomorfos, es compacto.

(d) El producto topológico de un conjunto de espacios mutuamente homeomorfos $\{(X_\alpha, \tau_\alpha)\}$, donde cada τ_α tiene tres elementos es compacto en la topología producto.

DEMOSTRACIÓN:

En el ejemplo anterior se demuestra que el Axioma de Elección implica el Teorema de Tychonoff. Por otra parte, es claro que el Teorema de Tychonoff implica *(c)* y *(c)* implica *(d)*. Así entonces, basta mostrar que *(d)* implica el Axioma de Elección; para ello emplearemos la equivalencia del Ejercicio 8.2.8.

Sean $\{X_\alpha\}_{\alpha\in I}$ una familia de conjuntos equipotentes y

$$a \notin \bigcup_{\alpha\in I} X_\alpha.$$

Para cada $\alpha \in I$, sea $Y_\alpha = X_\alpha \cup \{a\}$, y defina $\tau_\alpha = \{\emptyset, Y_\alpha, \{a\}\}$. Entonces

$$\{(Y_\alpha, \tau_\alpha)\}_{\alpha\in I}$$

satisface las hipótesis de *(d)*. Sea $W = \prod_{\alpha\in I} Y_\alpha$ con la topología producto y defina

$$Z_\alpha = \{f \in W : f(\alpha) \in X_\alpha\}.$$

Entonces $\{Z_\alpha\}_{\alpha\in I}$ es una familia de cerrados con la propiedad de la intersección finita. Consecuentemente,

$$\bigcap_{\alpha\in I} Z_\alpha = \prod_{\alpha\in I} X_\alpha$$

es no vacío. ■

Otro de los teoremas esenciales de la Topología que necesita del Axioma de Elección para demostrarse es el siguiente.

Ejemplo 8.29 (Lema de Urysohn) Cerrados ajenos en un espacio topológico normal están completamente separados. [2]

[2]Läuchli construyó en 1962 un modelo en el cual falla el Axioma de Elección y que contiene un espacio Hausdorff, normal y localmente compacto X con más de un punto, donde toda función continua $f : X \to \mathbf{R}$ es constante. Se sigue que el Lema de Urysohn no puede demostrarse sin el Axioma de Elección, y de hecho, que un espacio Hausdorff y compacto no necesariamente es normal.

Por completamente separados entendemos que existe una función continua con valores reales que manda a un conjunto al 0 y el otro al 1.

Sin demostración presentamos el siguiente teorema que establece otras equivalencias del Axioma de Elección.

Teorema 8.30 *El Axioma de Elección es equivalente a las siguientes proposiciones:*

(a) Sea $n \geq 2$ y sea $\mathcal{A}$ una familia de conjuntos infinitos. Entonces hay una función f tal que para cada $A \in \mathcal{A}$, $f(A)$ es una partición de A en conjuntos de cardinalidad entre 2 y n (Sierpiński, 1965; Levy, 1962).

(b) Si $m \geq 1$ y $\mathcal{A}$ es una familia de conjuntos no vacíos, entonces hay una función f tal que para cada $A \in \mathcal{A}$, $f(A)$ es un subconjunto no vacío de A con $|f(A)| \leq m$. (Levy, 1915)

(c) Si R es un orden parcial en un conjunto no vacío X y si cualquier subconjunto que es bien ordenado por R tiene una cota superior, entonces X tiene un elemento R-maximal (Kneser, 1950; Szele 1950).

Finalmente dos consecuencias del Axioma de Elección que contrastan con la intuición.

Ejemplo 8.31 (Teorema de Hausdorff) Una esfera S puede escribirse como unión de conjuntos ajenos A, B, C, Q tales que A, B y C son congruentes entre sí, $B \cup C$ es congruente a cada uno de los conjuntos A, B, C y Q es numerable.

Aquí por congruente debe entenderse que existe un movimiento rígido de $\mathbf{R}^3$ que transforma uno en el otro. Ahora considérese la siguiente relación entre subconjuntos de $\mathbf{R}^3$: Se define

$$X \approx Y \tag{8.4.2}$$

si existe una partición finita de X, $\{X_i\}_{i=0}^n$, y una partición del mismo número de elementos $\{Y_i\}_{i=0}^n$ de Y, tal que cada X_i es congruente a Y_i para cada $i \in \{0, 1, \ldots, n\}$.

Ejemplo 8.32 (Teorema de Banach-Tarski) Cualquier bola compacta D en $\mathbf{R}^3$ puede descomponerse en conjuntos ajenos U y V tales que

$$D \approx U \qquad D \approx V.$$

Así, usando el Axioma de Elección, uno puede cortar una bola en una cantidad finita de piezas y reacomodarlas para tener dos bolas del mismo tamaño a la original.

Los siguientes lemas establecerán las pruebas de estos dos teoremas. Sea G el producto libre de los grupos $\{1, \phi\}$ y $\{1, \psi, \psi^2\}$, es decir, el grupo de todos los productos formales de ϕ, ψ, ψ^2, con las relaciones $\phi^2 = 1$ y $\psi^3 = 1$. Consideraremos dos ejes de rotación a_ϕ, a_ψ a través del centro de la bola D, y consideraremos el grupo de rotaciones generado por la rotación ϕ de 180° alrededor de a_ϕ y una rotación ψ de 120° alrededor de a_ψ.

Lema 8.33 *Podemos determinar los ejes a_ϕ y a_ψ de tal modo que los distintos elementos de G representen distintas rotaciones generadas por ϕ y ψ.*

Un esbozo de la demostración es como sigue: Tenemos que determinar el ángulo θ entre a_ϕ y a_ψ de tal modo que ningún elemento de G distinto de 1 represente la rotación identidad. Considere un elemento típico de G; o sea, un producto del tipo

$$\alpha = \phi \cdot \psi^{\pm 1} \cdot \cdots \cdot \phi \cdot \psi^{\pm 1}. \tag{8.4.3}$$

Usando las ecuaciones de transformaciones ortogonales y algo de trigonometría elemental, uno puede probar que la ecuación

$$\alpha = 1,$$

donde α es algún producto del tipo (8.4.3), tiene sólo una cantidad finita de soluciones. Consecuentemente, excepto para un conjunto numerable de valores, tenemos libertad para seleccionar el ángulo θ que satisfaga el requerimiento.

Consideremos tal θ, y sea G el grupo de todas las rotaciones generadas por ϕ y ψ.

Lema 8.34 *El grupo G puede descomponerse en tres conjuntos ajenos*

$$G = A' \cup B' \cup C'$$

tales que

$$A' \cdot \phi = B' \cup C', \qquad A' \cdot \psi = B', \qquad A' \cdot \psi^2 = C'. \tag{8.4.4}$$

Demostración:

Construiremos A', B', C' por recursión sobre las longitudes de los elementos de G. Sea $1 \in A'$, $\phi, \psi \in B'$ y $\psi^2 \in C'$ y entonces continúe como sigue para cada $\alpha \in G$:

$$\alpha \text{ finaliza con } \begin{cases} \psi^{\pm 1}: & \begin{array}{ccc} \alpha \in A' & \alpha \in B' & \alpha \in C' \\ \hline \alpha\phi \in B' & \alpha\phi \in A' & \alpha\phi \in A' \end{array} \\ \phi: & \begin{cases} \alpha\psi \in B' & \alpha\psi \in C' & \alpha\psi \in A' \\ \alpha\psi^{-1} \in C' & \alpha\psi^{-1} \in A' & \alpha\psi^{-1} \in B' \end{cases} \end{cases}$$

Esto garantiza que la condición (8.4.4) se satisface. ■

Hasta ahora, no hemos hecho uso del Axioma de Elección. Para completar la demostración del Teorema de Hausdorff, usaremos un argumento similar a la construcción de un conjunto no medible de números reales.

Sea Q el conjunto de todos los puntos fijos sobre la esfera S de todas las rotaciones $\alpha \in G$. Cada rotación tiene dos puntos fijos; así Q es numerable. El conjunto $S \setminus Q$ es unión de conjuntos ajenos, a saber, de todas las órbitas P_x del grupo G:

$$P_x = \{x \cdot \alpha : \alpha \in G\}.$$

Por el Axioma de Elección, hay un conjunto M tal que contiene exactamente un elemento de cada P_x, $x \in S \setminus Q$. Si hacemos

$$A = M \cdot A', \qquad B = M \cdot B', \qquad C = M \cdot C',$$

se sigue de (8.4.4) que A, B, C son ajenos, congruentes entre sí y $B \cup C$ es congruente a ellos; más aún,

$$S = A \cup B \cup C \cup Q.$$

Esto completa la demostración del Teorema de Hausdorff. ■

Lema 8.35 *Sea $\approx$ la relación definida en (8.4.2). Entonces:*

(a) $\approx$ es una relación de equivalencia.

(b) Si X y Y son uniones ajenas de X_1, X_2 y Y_1, Y_2, respectivamente, y $X_i \approx Y_i$ para $i \in \{1, 2\}$, entonces $X \approx Y$.

(c) Si $X_1 \subseteq Y \subseteq X$ y si $X \approx X_1$ entonces $X \approx Y$.

Demostración:

Las pruebas de *(a)* y *(b)* no son difíciles. Para probar *(c)*, sean $X = \bigcup_{i=1}^{n} X_i$ y $X_1 = \bigcup_{i=1}^{n} X_{1i}$ tal que X_i es congruente a X_{1i} para cada $i \in \{1, \ldots, n\}$. Seleccione una congruencia $f_i : X_i \to X_{1i}$ para cada i, y sea $f : X \to X_1$ la función que coincide con f_i en cada X_i. Ahora sean

$$X_0 = X, \;\; X_1 = f(X_0), \;\; X_2 = f(X_1), \;\; \ldots$$

$$Y_0 = Y, \;\; Y_1 = f(Y_0), \;\; Y_2 = f(Y_1), \;\; \ldots$$

Si hacemos $Z = \bigcup_{n=0}^{\infty}(X_n \setminus Y_n)$, entonces $f(Z)$ y $X \setminus Z$ son ajenos, $Z \approx f(Z)$ y

$$X = Z \cup (X \setminus Z), \quad Y = f(Z) \cup (X \setminus Z).$$

Por lo tanto, $X \approx Y$ por (b). ■

Ahora probaremos el Teorema de Banach-Tarski. Sea D una bola compacta y sea

$$S = A \cup B \cup C \cup Q$$

la descomposición de la superficie garantizada por el Teorema de Hausdorff. Tenemos que

$$D = A^* \cup B^* \cup C^* \cup Q^* \cup \{c\}, \tag{8.4.5}$$

donde c es el centro de la bola y para cada $X \subseteq S$, X^* es el conjunto de todos los $x \in D$, distintos de c, tales que su proyección sobre la superficie está en X. Claramente,

$$A^* \approx B^* \approx C^* \approx B^* \cup C^*. \tag{8.4.6}$$

Sean

$$U = A^* \cup Q^* \cup \{c\}, \qquad V = B \setminus U.$$

De (8.4.6) y del Lema 8.35, tenemos que

$$A^* \approx A^* \cup B^* \cup C^*, \tag{8.4.7}$$

y así

$$U \approx D.$$

Ahora es fácil encontrar alguna rotación α (no en G) tal que Q y $Q \cdot \alpha$ sean ajenos, y así, usando $C^* \approx A^* \cup B^* \cup C^*$, existe $S \subseteq C$ tal que $S^* \approx Q^*$. Sea p algún punto en $S \setminus C$. Obviamente,

$$A^* \cup Q^* \cup \{c\} \approx B^* \cup S^* \cup \{p\}.$$

Como

$$B^* \cup S^* \cup \{p\} \subseteq V \subseteq D,$$

podemos hacer uso de la relación $U \approx B$ y del Lema 8.35(c), para obtener

$$V \approx D.$$

Esto completa la demostración. ■

Los Teoremas de Hausdorff y Banach-Tarski tienen generalizaciones a dimensiones superiores; sin embargo, son falsos para dimensiones 1 y 2. Estos teoremas están íntimamente relacionados con el problema de la medida, además de tener consecuencias propias. El lector interesado puede consultar [W_1].

8.5 El Teorema del Ideal Primo

En los ejemplos de la sección precedente, mostramos que usando el Axioma de Elección, podemos establecer la existencia de ideales maximales en anillos, retículas o álgebras de conjuntos. Entre los teoremas de este tipo, el Teorema del Ideal Primo juega un papel particularmente predominante. Primeramente, porque puede ser usado en muchas demostraciones en lugar del Axioma de Elección; en segundo lugar, porque es equivalente a muchas otras proposiciones; y finalmente, porque es esencialmente más débil que el Axioma de Elección.

Definición 8.36 Un *álgebra booleana* es un conjunto B con dos operaciones binarias $+$ y $\cdot$ (suma y multiplicación booleanas), una operación unitaria $-$ (complemento) y dos constantes $1, 0$ que cumplen las siguientes condiciones:

(a) $u + u = u = u \cdot u$;
(b) $u + v = v + u$ y $u \cdot v = v \cdot u$;
(c) $u + (v + w) = (u + v) + w$ y $u \cdot (v \cdot w) = (u \cdot v) \cdot w$;
(d) $(u + v) \cdot w = (u \cdot w) + (v \cdot w)$ y $(u \cdot v) + w = (u + w) \cdot (v + w)$;
(e) $u + (u \cdot v) = u = u \cdot (u + v)$
(f) $u + (-u) = 1$ y $u \cdot (-u) = 0$;
(g) $-(u + v) = -u \cdot -v$ y $-(u \cdot v) = -u + -v$;
(h) $-(-u) = u$;
(i) $u \cdot 1 = u$ y $u + 0 = u$.

Se puede introducir un orden (parcial) $\leq$ de manera natural en una álgebra booleana B el cual se introduce en términos de $+$ por

$$u \leq v \quad \text{si y sólo si} \quad u + v = v$$

o equivalentemente

$$u \leq v \quad \text{si y sólo si} \quad u \cdot v = u.$$

Con este orden, 1 y 0 son el máximo y el mínimo de B, respectivamente. Además, $u + v$ y $u \cdot v$ representan el supremo y el ínfimo de $\{u, v\}$, respectivamente.

En el Ejercicio 4.5.20 se definió a una retícula como un conjunto parcialmente ordenado $(L, \leq)$ tal que para cada $a, b \in L$ existen

$$a \perp b = \inf\{a, b\} \qquad \text{y} \qquad a \top b = \sup\{a, b\}.$$

Con lo anterior, se puede describir un álgebra booleana como una retícula $(B, \leq)$ con elementos máximo y mínimo, que es distributiva y cada elemento tiene un complemento, es decir,

$$\begin{gathered}(a \top b) \bot c = (a \bot c) \top (b \bot c), \\ (a \bot b) \top c = (a \top c) \bot (b \top c), \\ \forall a \in L,\, \exists\, b \in L \text{ tal que } a \top b = \max B,\ a \bot b = \min B.\end{gathered}$$

Ejemplo 8.37 Para cualquier conjunto X, $\mathcal{P}(X)$ con $\cup$ como suma, $\cap$ como multiplicación y $X \setminus A$ como el complemento $-A$ de $A \in \mathcal{P}(X)$ es un álgebra booleana. Aquí $\leq$ es simplemente la inclusión de conjuntos.

Ejemplo 8.38 Salvo que X sea finito, la retícula de todos los subconjuntos finitos de X con la contención es distributiva pero no es un álgebra booleana.

Definición 8.39 Un *ideal* I en un álgebra booleana B es un subconjunto no vacío de B tal que:

(a) $u \in I$ y $v \leq u$ implica $v \in I$;
(b) $u, v \in I$ implica $u + v \in I$.

Antes de dar ejemplos de ideales observe que cualquier ideal I contiene a 0.

Ejemplo 8.40 $\{0\}$ es el $\subseteq$-mínimo ideal en cualquier álgebra Booleana B y $I = B$ es el $\subseteq$-máximo ideal. A estos ideales les llamaremos *trivial e impropio*, respectivamente; todos los otros ideales se llaman *propios*.

Ejemplo 8.41 Un ideal I, no trivial, es propio si y sólo si $1 \notin I$.

Ejemplo 8.42 En cualquier álgebra booleana, si $u \in B$, entonces

$$\{v \in B : v \leq u\}$$

es un ideal, llamado *ideal principal* generado por $u \in B$.

Ejemplo 8.43 En $\mathcal{P}(X)$ la familia $\mathcal{I}$ de todos los subconjuntos finitos de X es un ideal.

Definición 8.44 Un ideal propio I se llama *primo* si siempre que $u \cdot v \in I$ se tiene que $u \in I$ o $v \in I$.

Se deduce fácilmente que si I es un ideal primo, entonces para cada $u \in B$, o bien $u \in I$, o $-u \in I$ (pues $u \cdot -u = 0$). El recíproco también es cierto, es decir, si I es un ideal propio tal que para cualquier $u \in B$, $u \in I$, o $-u \in I$,

entonces I es un ideal primo. En efecto, si $u \cdot v \in I$, pero $u \notin I$, $v \notin I$, entonces $-u, -v \in I$, luego $-(u \cdot v) = -u + -v \in I$, de aquí que

$$1 = (u \cdot v) + -(u \cdot v) \in I;$$

lo que contradice que I sea un ideal propio.

Proposición 8.45 *En un álgebra booleana, un ideal I es primo si y sólo si es $\subseteq$-maximal en la familia de ideales propios, es decir, I no está contenido propiamente en algún ideal propio.*

DEMOSTRACIÓN:

$\Leftarrow$] Sea I un ideal $\subseteq$-maximal en la familia de todos los ideales propios de un álgebra booleana B. Para mostrar que I es un ideal primo basta probar que para cada $u \in B$, o bien $u \in I$ o $-u \in I$. Sea $u \in B$ y supongamos que $u \notin I$. Consideremos el siguiente subconjunto de B:

$$J = \{x + y : x \leq u, \quad y \in I\}.$$

Entonces J es un ideal en B ya que:

(a) Si $z \in B$ es tal que $z \leq x + y$ para algunos $x \leq u$, $y \in I$, entonces $z \cdot (x + y) = z \cdot x + z \cdot y$. Pero como $z \cdot x = \inf\{x, z\}$, $z \cdot x \leq x$ y dado que $x \leq u$, se sigue que $z \cdot x \leq u$. Además, dado que I es un ideal, $z \cdot y \leq y$ implica $z \cdot y \in I$. Por lo tanto, $z \in J$.

(b) Si $x_1 \leq u$, $x_2 \leq u$, $y_1, y_2 \in I$, entonces $x_1 + x_2 = \sup\{x_1, x_2\} \leq u$ y $y_1 + y_2 \in I$, luego

$$(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in J.$$

También $I \subset J$, puesto que claramente $I \subseteq J$ y $u \in J$ mientras que $u \notin I$. Así $J = B$, dado que I es maximal. Por lo tanto, existen $x \leq u$, $y \in I$ tales que $x + y = 1$. De esto se concluye que $u + (x + y) = u + 1$ o bien $u + y = 1 + u = 1$. Entonces $-u = -u \cdot 1 = -u \cdot (u + y) = (-u \cdot u) + (-u \cdot y) = -u \cdot y$; o sea que $-u \leq y$. Se concluye que $-u \in I$.

$\Rightarrow$] Si I es un ideal primo y $I \subset J$, entonces existe $u \in J \setminus I$. Como I es primo, $-u \in I$, luego $1 = u + -u \in J$; o sea, $J = B$. ■

Hay nociones duales para ideal e ideal primo.

Definición 8.46 Un *filtro* F en un álgebra booleana es un subconjunto no vacío tal que:

(a) $u \in F$ y $u \leq v$ implica $v \in F$;

(b) $u \in F$ y $v \in F$ implica $u \cdot v \in F$.

$\{1\}$ y B son filtros en B, llamados *trivial e impropio*; a todos los demás filtros les llamaremos *propios*. También por dualidad, un filtro F, no trivial, es propio si y sólo si $0 \notin F$.

Ejemplo 8.47 La colección de conjuntos *co-finitos* (es decir, conjuntos con complemento finito) es un filtro en $\mathcal{P}(X)$ para cualquier conjunto (infinito) X.

Ejemplo 8.48 En cualquier álgebra booleana, si $u \in B$, entonces

$$\{v \in B : u \leq v\}$$

es un filtro, llamado el filtro *principal generado por* $u \in B$.

Ejemplo 8.49 Si $\mathcal{G} \subseteq \mathcal{P}(X)$ es una familia con la *propiedad de la intersección finita* (es decir, la intersección de cualquier subfamilia finita de $\mathcal{G}$ es no vacía), entonces existe un filtro propio $\mathcal{F}$ en $\mathcal{P}(X)$ que contiene a $\mathcal{G}$. En efecto, basta considerar a la familia $\mathcal{F}$ de todos los subconjuntos F de X con la propiedad de que existe un subconjunto finito $\{G_1, \ldots G_n\}$ de $\mathcal{G}$ tal que

$$G_1 \cap \ldots \cap G_n \subseteq F.$$

Definición 8.50 Un filtro propio F se llama *ultrafiltro* si siempre que $u + v \in F$ implica que $u \in F$ o $v \in F$.

También para un filtro propio F son equivalentes:

(a) F es un ultrafiltro,

(b) Para cada $u \in B$, $u \in F$ o $-u \in F$,

(c) F es $\subseteq$-maximal en la familia de todos los filtros propios.

Ejemplo 8.51 Sea $x \in \mathbf{R}$, y sea $\mathcal{F}$ la colección de todos los subconjuntos $V \subseteq \mathbf{R}$ tales que

$$x \in (x - \epsilon, x + \epsilon) \subseteq V$$

para algún $\epsilon > 0$. $\mathcal{F}$ es un filtro propio en $\mathcal{P}(\mathbf{R})$; pero no es un ultrafiltro ya que ni $\{x\}$, ni $\mathbf{R} \setminus \{x\}$ son elementos de $\mathcal{F}$.

Lema 8.52 *Si* $\{I_\alpha\}_\alpha$ *es una* $\subseteq$*-cadena de ideales en un álgebra Booleana* B *tales que* $u_0 \in B \setminus I_\alpha$ *para cada* α*, entonces* $\bigcup_\alpha I_\alpha$ *es un ideal en* B *que no contiene a* u_0.

DEMOSTRACIÓN:

(a) Si $u \in I = \bigcup_\alpha I_\alpha$ y $v \leq u$, entonces $u \in I_\alpha$ para algún α. Como I_α es un ideal, $v \in I_\alpha \subseteq I$.

(b) Si $u, v \in I$, entonces existen α_1, α_2 tales que $u \in I_{\alpha_1}$ y $v \in I_{\alpha_2}$. Como $\{I_\alpha\}_\alpha$ es una $\subseteq$-cadena, podemos suponer sin pérdida de generalidad que $I_{\alpha_1} \subseteq I_{\alpha_2}$; así, $u + v \in I_{\alpha_2} \subseteq I$.

Es claro que $u_0 \notin I$. ■

Teorema 8.53 (del Ideal Primo) *Toda álgebra booleana tiene un ideal primo.*

DEMOSTRACIÓN:

Sean B un álgebra booleana y $u \in B$ un elemento fijo. Consideremos la familia $\mathcal{I}$ de todos los ideales en B que no contienen a u; por el lema anterior, la familia $\mathcal{I}$ ordenada por contención cumple las hipótesis del Lema de Kuratowski-Zorn; así $\mathcal{I}$ tiene un elemento maximal I, este ideal es un ideal primo. ■

El Teorema del Ideal Primo es una consecuencia fácil del Axioma de Elección, pero J. D. Halpern demostró que el recíproco es falso, es decir, el Axioma de Elección no puede demostrarse a partir del Teorema del Ideal Primo. En esta sección veremos algunas equivalencias del Teorema del Ideal Primo. Primero note que el Teorema 8.53 es equivalente a una versión aparentemente más fuerte.

Teorema 8.54 *En cualquier álgebra booleana, todo ideal propio puede extenderse a un ideal primo.*

Para mostrar que la versión más fuerte se sigue de la versión débil, tomemos B un álgebra booleana B e I un ideal en B. Considere la relación de equivalencia

$$u \sim v \qquad \text{si y sólo si} \qquad (u \cdot -v) + (v \cdot -u) \in I.$$

Sea C el conjunto de todas las clases de equivalencia $[u]$ y defina operaciones $+, \cdot$ y $-$ sobre C como sigue:

$$[u] + [v] = [u + v]\,, \qquad [u] \cdot [v] = [u \cdot v]\,, \qquad -[u] = [-u]\,.$$

Entonces C es un álgebra booleana, llamada *cociente* de B. Por el Teorema del Ideal Primo, C tiene un ideal primo K. No es difícil verificar que el conjunto

$$J = \{u \in B : [u] \in K\}$$

es un ideal primo en B y que $I \subseteq J$.

Usando la dualidad entre ideales y filtros, tenemos las siguientes formulaciones del Teorema del Ideal Primo.

Teorema 8.55 *Son equivalentes al Teorema del Ideal Primo:*

(a) Toda álgebra booleana tiene un ultrafiltro.

(b) Cualquier filtro propio en un álgebra booleana puede extenderse a un ultrafiltro.

Un caso especial de álgebra booleana es el conjunto $\mathcal{P}(X)$ con las operaciones conjuntistas $\cup$, $\cap$, $\setminus$; el concepto de filtro y ultrafiltro coinciden con las definiciones anteriores (ver después del Teorema de Tychonoff).

Teorema 8.56 (del Ultrafiltro) *Todo filtro sobre un conjunto X puede extenderse a un ultrafiltro.*

Tenemos demostrado que el Teorema del Ultrafiltro es equivalente al Teorema del Ideal Primo. Sin embargo, la correspondiente versión más débil del Teorema del Ultrafiltro: *Cada conjunto no vacío X tiene un ultrafiltro sobre X*, es trivialmente cierta sin usar el Axioma de Elección. En efecto, sea $x \in X$, entonces el filtro principal generado por $\{x\}$,

$$\mathcal{F}_x = \{Y \subseteq X : x \in Y\}$$

claramente es un ultrafiltro sobre X. Sin embargo, la proposición: *Cada conjunto infinito X tiene un ultrafiltro no principal*, no es obvia. S. Feferman mostró en 1964 que es consistente con los axiomas **ZF** que todo ultrafiltro en **N** sea principal. Posteriormente A. Blass en 1977 [B_2], modificando el método de Feferman, probó que también es consistente con los axiomas **ZF** que todo ultrafiltro sobre un conjunto X sea principal. De lo anterior se deduce que sin el Axioma de Elección la proposición anterior es indemostrable. Pero puede probarse que es esencialmente una versión más débil que el Teorema del Ideal Primo (ver [J_2, pag. 132, problema 5]). Un buen ejemplo del empleo de la proposición anterior lo dio Sierpiński en 1938 al mostrar que se pueden construir subconjuntos no medibles de **R** según Lebesgue si se acepta la existencia de ultrafiltros libres sobre **N**. El resultado de Sierpiński fue mejorado por Z. Samadeni en [S_1].

Ahora daremos ejemplos del uso del Teorema del Ideal Primo.

Una familia $\mathcal{A}$ de subconjuntos de un conjunto dado S es un *álgebra de conjuntos* si:

$$S \in \mathcal{A},$$

$X, Y \in \mathcal{A}$ implica $X \cup Y \in \mathcal{A}$, $X \cap Y \in \mathcal{A}$,
$X \in \mathcal{A}$ implica $S \setminus X \in \mathcal{A}$.

Un *homomorfismo* entre álgebras booleanas B_1 y B_2 es una función $\Phi : B_1 \to B_2$ que preserva las operaciones de suma, multiplicación y complemento de las álgebras B_1 y B_2. Un homomorfismo biyectivo se llama *isomorfismo.* Si existe un isomorfismo las álgebras se dicen *isomorfas.*

Ejemplo 8.57 (Teorema de Representación de Stone) Toda álgebra booleana es isomorfa a un álgebra de conjuntos.

Demostración:

Sea B un álgebra booleana; sea

$$\mathcal{S} = \{U : U \text{ es un ultrafiltro en } B\}.$$

Para cada $u \in B$, sea $\Phi(u) = \{U \in S : u \in U\}$. Es fácil ver que

$$\begin{gathered}\Phi(u+v) = \Phi(u) \cup \Phi(v),\\ \Phi(u \cdot v) = \Phi(u) \cap \Phi(v),\\ \Phi(-u) = \mathcal{S} \setminus \Phi(u).\end{gathered}$$

Si $u \neq v$, entonces $u \not\leq v$ o $v \not\leq u$. Supongamos que $u \not\leq v$, un argumento similar se sigue si $v \not\leq u$. Si $u \cdot (-v) = 0$, entonces

$$v = v + 0 = v + (u \cdot (-v)) = (u + v) \cdot (v + (-v)) = (u + v) \cdot 1 = u + v;$$

o sea $u \leq v$. Por lo tanto, $u \cdot (-v) \neq 0$. Sea $F = \{w \in B : u \cdot (-v) \leq w\}$ el filtro principal generado por $u \cdot (-v)$. Claramente F es un filtro propio; por el Teorema 8.55(b), F puede extenderse a un ultrafiltro U.

Ahora $-(u \cdot (-v)) = -u + v \notin U$, lo cual implica que $U \notin \Phi(-u + v) = \Phi(-u) \cup \Phi(v)$, por lo que $U \in \Phi(u)$ y $U \notin \Phi(v)$. Esto establece la inyectividad de Φ. Así, Φ es un isomorfismo de B sobre $\Phi(B)$. ■

Es un hecho notable que el Teorema de Representación de Stone es equivalente al Teorema del Ideal Primo.

Teorema 8.58 *El Teorema de Representación de Stone implica el Teorema del Ideal Primo.*

Demostración:

Sean B un álgebra booleana, $\mathcal{F}$ un álgebra de conjuntos isomorfa a B y $\Phi : B \to \mathcal{F}$ un isomorfismo. Tomemos $p \in \bigcup \mathcal{F}$ y sea

$$U = \{u \in B : p \in \Phi(u)\}.$$

No es difícil mostrar que U es un ideal primo en B. ■

El Teorema del Ideal Primo también implica una cuestión indecidible en **ZF**, a saber, cualquier conjunto puede ser totalmente ordenado. De hecho, a partir del Teorema del Ideal Primo se puede demostrar el Principio de Extensión de Orden que aparece en el siguiente ejemplo y que evidentemente es más fuerte que la proposición que asegura la existencia de un orden lineal para cualquier conjunto; sin embargo, el Principio de Extensión de Orden no implica el Teorema del Ideal Primo (ver [J_2, sección 7.2, problemas 7.8 y 5.27]). Si $\leq$ y $\preceq$ son órdenes (parciales) de un conjunto P, entonces se dice que $\preceq$ *extiende* a $\leq$ si para cualesquiera $p, q \in P$, $p \leq q$ implica $p \preceq q$.

Ejemplo 8.59 (Principio de Extensión de Orden) Todo orden (parcial) de un conjunto P puede extenderse a un orden lineal de P.

Como una aplicación del Teorema del Ideal Primo al Álgebra tenemos el siguiente. Un campo F es un *campo ordenado* si hay un orden lineal $\leq$ en F que satisface:

(i) Si $a \leq b$, entonces $a + c \leq b + c$ para todo c;
(ii) Si $a \leq b$ y $c \geq 0$, entonces $a \cdot c \leq b \cdot c$.

Ejemplo 8.60 (Teorema de Artin-Schreir) Todo campo en el que -1 no es suma de cuadrados puede ser ordenado.

Ejemplo 8.61 El Teorema del Ideal Primo implica que cualquier producto topológico de espacios compactos de Hausdorff es no vacío.

Ejemplo 8.62 El Teorema del Ideal Primo implica que cualquier producto topológico de espacios compactos de Hausdorff es compacto.

Otra equivalencia al Teorema del Ideal primo es una versión débil del Teorema de Tychonoff.

Teorema 8.63 *El Teorema del Ideal Primo es equivalente a la siguiente proposición: El producto topológico de cualquier familia de espacios discretos con dos puntos cada uno, es compacto.*

Ejemplo 8.64 El Teorema del Ideal Primo implica el Teorema de Compactación de Stone-Čech.

Ejemplo 8.65 El Teorema del Ideal Primo implica el Teorema de Hahn-Banach.

Podemos decir más al respecto. Una *medida* (de valores reales) en un álgebra booleana es una función no negativa $\mu : B \to \mathbf{R}$ tal que $\mu(0) = 0$, $\mu(1) = 1$, y $\mu(a + b) = \mu(a) + \mu(b)$ siempre que $a \cdot b = 0$. El Teorema de Hahn-Banach es equivalente a la afirmación de que toda álgebra booleana admite una medida con valores reales.

La demostración del Teorema de Hahn-Banach a partir del Teorema del Ideal Primo fue dada por J. Łos y C. Ryll-Nardzewski. Otra versión de la prueba la dio W. A. J. Luxemburg. La equivalencia antes asegurada se debe a Ryll-Nardzewski y Luxemburg.

Ejercicios 8.5

1. Verifique las afirmaciones de los Ejemplos 8.38, 8.41, 8.42, 8.47, y 8.48.

2. (a) Supóngase que $\mathcal{F}$ es un ultrafiltro sobre un conjunto X y sea $A \in \mathcal{F}$. Demuestre que si $B \subseteq A$, entonces $B \in \mathcal{F}$ o $A \setminus B \in \mathcal{F}$.

   (b) Si $\mathcal{F}$ es un ultrafiltro sobre un conjunto X y

   $$X = A_1 \cup A_2 \cup \cdots \cup A_n.$$

   Muestre que para algún $i \in \{1, \ldots, n\}$, $A_i \in \mathcal{F}$.

   (c) Pruebe que si X es un conjunto finito, entonces cualquier ultrafiltro sobre X es principal.

3. Demuestre que si $\mathcal{U}$ es un ultrafiltro no principal sobre un conjunto X, entonces cualquier $U \in \mathcal{U}$ es infinito.

4. Muestre que si I es un álgebra booleana B, entonces $B \setminus I$ es un filtro en B.

5. Complete la demostración de la equivalencia entre el Teorema del Ideal Primo y el Teorema de Representación de Stone.

6. (a) Muestre que hay una correspondencia biyectiva entre los ideales y los filtros en un álgebra booleana.

   (b) Muestre que hay una correspondencia biyectiva entre los ideales primos y los ultrafiltros en un álgebra booleana.

7. Supóngase que $f : B_1 \to B_2$ es un homomorfismo de álgebras booleanas. Pruebe que si J es un ideal (respectivamente, un filtro) en B_2, entonces $f^{-1}(J)$ es un ideal (respectivamente, un filtro) en B_1. En particular $I(f) = f^{-1}(\{0\})$ es un ideal primo en B_1 llamado *núcleo* de f; $F(f) = f^{-1}(\{1\})$ es un ultrafiltro en B_2 llamado el *co-núcleo* de f.

8. Sea $\mathcal{U}$ un ultrafiltro sobre un conjunto X, y sea $f : X \to Y$ una función. Muestre que
$$f^{\#}\mathcal{U} = \left\{V \subseteq Y : f^{-1}(V) \in \mathcal{U}\right\}$$
es un ultrafiltro sobre Y.

9. Sea B un álgebra booleana. Para cada $u \in B$, sean:
$$I_u = \{x \in B : u \cdot x = 0\},$$
$$F_u = \{x \in B : u + x = 1\}.$$
Muestre que estos conjuntos son, respectivamente, un ideal y un filtro en B.

10. Demuestre que si F es un filtro en B, entonces el mínimo filtro que contiene a $F \cup \{u\}$ es
$$\{y \in B : \exists\, x \in F \text{ tal que } y \geq x \cdot u\}.$$

11. Un *carácter* de un álgebra booleana B es un homomorfismo $\varphi : B \to 2$. La colección de todos los carácteres de B se llama *espectro* de B y es denotado por $spec(B)$ Pruebe que:

    (a) Hay una correspondencia biyectiva entre $spec(B)$ y la familia de ultrafiltros en B dada por $\varphi \mapsto F(\varphi)$.

    (b) Hay una correspondencia biyectiva entre $spec(B)$ y la familia de todos los ideales primos en B dada por $\varphi \mapsto I(\varphi)$.

    (c) La función $\Phi : B \to \mathcal{P}(spec(B))$ definida por
    $$\Phi(u) = \{\varphi \in spec(B) : f(u) = 1\}$$
    es un homomorfismo entre álgebras booleanas.

12. Demuestre que la siguiente proposición es equivalente al Teorema del Ideal Primo: Si B es un álgebra booleana y $S \subseteq B$ es tal que $0 \notin S$ y S es cerrado con respecto a $\cdot$, entonces existe un ideal $\subseteq$-maximal ajeno a S. (Sugerencia: para la necesidad considere $J = \{u \in B : \exists\, v \in S,\ u \leq -v\}$, muestre que J es un ideal propio y aplique el Teorema 8.54. Para la suficiencia considere $S = \{1\}$.)

13. En este Ejercicio se establece la equivalencia del Teorema del Ideal Primo con versiones débiles del Teorema de Tychonoff.

    (a) Si $\mathcal{U}$ es un ultrafiltro sobre un espacio Hausdorff, pruebe que la intersección $\bigcap \{\overline{A} : A \in \mathcal{U}\}$ contiene a lo más un punto.

    (b) Demuestre que el Teorema del Ultrafiltro implica que cualquier producto de espacios Hausdorff compactos es no vacío. (Sugerencia: sea $X = \prod_{\alpha \in I} X_\alpha$. Sea $\mathcal{Z}$ el conjunto de todos las funciones f con $dom\, f \subseteq I$ y $f(\alpha) \in X_\alpha$, y sea $\mathcal{Z}_\alpha = \{f \in \mathcal{Z} : \alpha \in dom\, f\}$ para cada $\alpha \in I$. Sea $\mathcal{F}$ el filtro generado en $\mathcal{Z}$ por $\mathcal{Z}_\alpha,\ \alpha \in I$, y sea $\mathcal{U} \supseteq \mathcal{F}$ un ultrafiltro. Sea $\mathcal{U}_\alpha$ la proyección de $\mathcal{U}$ sobre X_α. Para cada $\alpha \in I$, la intersección
    $$\bigcap \{\overline{A} : A \in \mathcal{U}_\alpha\}$$
    contiene exactamente un punto $x_\alpha \in X_\alpha$.)

    (c) Demuestre que el Teorema del Ultrafiltro implica que cualquier producto topológico de espacios Hausdorff compactos, es compacto. (Sugerencia: el producto es no vacío por el inciso anterior. En la demostración del Teorema de Tychonoff en la Sección 8.4, la primera parte usa únicamente el Teorema del Ultrafiltro. El uso del Axioma de Elección en el punto (2) es eliminado por el inciso (a).)

    (d) Demuestre que la siguiente proposición implica el Teorema del Ideal Primo: El producto topológico de cualquier familia de espacios discretos con dos puntos cada uno es compacto. (Sugerencia: sea B un álgebra booleana, y sea $X = \prod \{\{u, -u\} : u \in B\}$. Para una subálgebra finita A de B y un ideal primo I en A, sean
    $$X_I = \{x \in X : x(u) \in I \text{ para cada } u \in A\}$$
    y $X_A = \bigcup \{X_I : I \text{ es un ideal primo en } A\}$. La familia
    $$\{X_A : A \text{ es una subálgebra finita}\}$$
    es una base de filtro de conjuntos cerrados; de su intersección se obtiene un ideal primo en B.)

(e) Demuestre que la siguiente proposición implica el Teorema del Ideal Primo: El espacio generalizado de Cantor $\{0,1\}^I$ es compacto para cualquier I. (Sugerencia: use esto para demostrar la proposición del inciso (c). Es suficiente mostrar que cualquier producto de conjuntos de dos elementos cada uno, es no vacío. Sea S un conjunto de pares (no ordenados) ajenos $p = \{a, b\}$ y sea $I = \bigcup\{p : p \in S\}$. En el producto $\{0,1\}^I$, los conjuntos $X_p = \{f : f(a) \neq f(b) \text{ si } p = \{a, b\}\}$ son cerrados y forman una base de filtro. La intersección proporciona una función de elección para S.)

14. Use el ejercicio anterior y establezca el Teorema de la Compactación de Stone-Čech. (Sugerencia: βX es un subconjunto de $[0,1]^X$.)

8.6 Otras Proposiciones Relacionadas.

Con frecuencia, especialmente cuando se trabaja con conjuntos de números reales, no es necesario usar en plenitud el Axioma de Elección y de hecho es mucho más usada una débil variación de éste.

Axioma de Elecciones Numerables *Para cualquier familia numerable de conjuntos no vacíos* $\{A_n\}_{n\in\mathbf{N}}$ *existe una función* $f : \mathbf{N} \to \bigcup_{n=0}^{\infty} A_n$ *tal que* $f(n) \in A_n$.

Con el Axioma de Elecciones Numerables, pueden demostrarse muchas proposiciones extremadamente útiles en el Análisis Matemático, los Ejemplos 8.15, 8.16 y 8.17 pueden demostrarse con él.

Teorema 8.66 *Las siguientes afirmaciones son equivalentes:*

(a) El Axioma de Elecciones Numerables.

(b) Si $\{A_n\}_{n\in\mathbf{N}}$ *es una familia de conjuntos ajenos, entonces hay una sucesión* $(x_n)_{n=0}^{\infty}$ *tal que* $x_n \in A_n$ *para cada* $n \in \mathbf{N}$.

(c) El producto cartesiano de una familia numerable de conjuntos no vacíos es no vacío.

En 1942, P. A. Bernays formuló el siguiente axioma que es una versión más débil que el Axioma de Elección pero más fuerte que el Axioma de Elecciones Numerables (las demostraciones de estas afirmaciones pueden encontrarse en [J$_2$]; la primera en el problema 26 de la página 85 y la segunda en la sección 8.2).

Axioma de Elección Dependiente *Si R es una relación en un conjunto no vacío X tal que para todo $x \in X$, existe $y \in X$ tal que xRy, entonces existe una sucesión $(x_n)_{n=0}^{\infty}$ tal que $x_n R x_{n+1}$.*

Teorema 8.67 *El Axioma de Elección Dependiente implica el Axioma de Elecciones Numerables.*

DEMOSTRACIÓN:

Sea $\{A_n\}_{n\in\mathbf{N}}$ una familia a lo más numerable de conjuntos no vacíos y sea X el conjunto de todas las sucesiones finitas $s = (a_i)_{i=0}^{k}$ tales que $a_0 \in A_0$, ..., $a_k \in A_k$. Definamos

$$s\,R\,t \quad \text{si y sólo si} \quad s = (a_i)_{i=0}^{k} \;\text{ y }\; t = (a_i)_{i=0}^{k+1}.$$

Aplicando el Axioma de Elección Dependiente se obtiene una sucesión $(a_n)_{n=0}^{\infty}$ tal que $a_n \in A_n$ para cada $n \in \mathbf{N}$. ■

Teorema 8.68 *Las siguientes afirmaciones son equivalentes:*

(a) El Axioma de Elección Dependiente.

(b) Todo conjunto linealmente ordenado que no contiene la imagen de una sucesión estrictamente decreciente es bien ordenado.

(c) Sea R una relación en A tal que para todo $x \in X$ existe $y \in X$ tal que xRy. Si $a \in A$, entonces hay una sucesión $(x_n)_{n=0}^{\infty}$ tal que $x_0 = a$ y $x_n\,R\,x_{n+1}$ para cada $n \in \mathbf{N}$.

DEMOSTRACIÓN:

(a) $\Rightarrow$ (b). Sea $(A, \leq)$ un conjunto parcialmente ordenado que no sea bien ordenado. Entonces existe un subconjunto de A, digamos B, tal que B no tiene un mínimo elemento. Ahora, el dominio del orden dual estricto, restringido a B, $>_B$, es B, de otro modo B tendría un elemento minimal. Por hipótesis, existe una sucesión $(y_n)_{n=0}^{\infty}$ en B tal que $y_n >_B y_{n+1}$ para todo $n \in \mathbf{N}$. Así, A contiene una sucesión estrictamente decreciente.

(b) $\Rightarrow$ (a). Sean R una relación en A y X el conjunto de todas las sucesiones finitas φ en A tales que

$$\varphi(0)\,R\,\varphi(1)\,R\,\varphi(2)\,R\cdots R\,\varphi(n-1)$$

(cuando $dom\,\varphi = n$). Definiendo $\preceq$ en X por $\varphi \preceq \psi$ si y sólo si $\varphi \supseteq \psi$, tenemos que $(X, \preceq)$ es un conjunto ordenado, el cual evidentemente no es bien ordenado. Empleando la hipótesis, existe una sucesión $(\varphi_n)_{n=0}^{\infty}$ estrictamente decreciente en X. Ahora, $\{\varphi_n : n \in \mathbf{N}\}$ es un sistema compatible de funciones,

por lo cual, $\varphi = \bigcup_{n=0}^{\infty} \varphi_n$ es una sucesión en A tal que $\varphi(n)\, R\, \varphi(n+1)$ para cada $n \in \mathbf{N}$.

(a) $\Rightarrow$ *(c).* Sean R una sucesión en A y $a \in A$. Considere

$$B = \bigcap \{C \subseteq A : a \in C \text{ y } R(C) \subseteq C\}.$$

Es fácil mostrar que el dominio de la restricción de R a B es B. Consecuentemente, por hipótesis, existe una sucesión $(y_n)_{n=0}^{\infty}$ en B tal que $y_n\, R\, y_{n+1}$ para cada $n \in \mathbf{N}$.

Por otra parte, también puede mostrarse que

$$B = \bigcup_{m=0}^{\infty} R^m(\{a\}),$$

donde $R^0 = Id_A$ y $R^{m+1} = R^m \circ R$. Así, $y_0 \in R^m(\{a\})$ para algún $m \in \mathbf{N}$, es decir, existe $\{z_0, z_1, \ldots, z_m\} \subseteq B$ tal que $z_0 = a$, $z_m = y_0$ y para cada $n < m$, $z_n\, R\, z_{n+1}$. Si hacemos

$$x_n = \begin{cases} z_n, & \text{para } n < m \\ y_{n-m}, & \text{para } n \geq m, \end{cases}$$

entonces es claro que $x_0 = a$ y $x_n\, R\, x_{n+1}$ para todo $n \in \mathbf{N}$.

(c) $\Rightarrow$ *(a).* Trivial. ■

Finalmente consideremos otras dos proposiciones más débiles que el Axioma de Elección.

Axioma de Elección para Conjuntos Finitos *Para cualquier familia no vacía $\mathcal{F}$ de conjuntos finitos no vacíos existe una función $f : \mathcal{F} \to \bigcup \mathcal{F}$ tal que $f(F) \in F$.*

Axioma de Elección n-Finito *Para cualquier familia no vacía $\mathcal{F}$ de conjuntos de n elementos existe una función $f : \mathcal{F} \to \bigcup \mathcal{F}$ tal que $f(F) \in F$.*

Renunciar parcialmente al Axioma de Elección y adoptar proposiciones alternativas no nos deja del todo desamparados, los ejemplos anteriores son una muestra importante de ello. Por otra parte, estas proposiciones, posibles sustitutas del Axioma de Elección, no traen consigo resultados tan paradójicos como el Axioma de Elección. Pero estos axiomas más débiles que el Axioma de Elección son insuficientes para las necesidades plenas de las matemáticas.

A continuación enlistamos las proposiciones alternativas al Axioma de Elección que hemos considerado y mostramos en un diagrama sus relaciones. Como

se dijo antes, el Axioma de Elección puede sustituirse por estas u otras proposiciones, y es interesante saber el alcance de estas Teorías de Conjuntos "no estándar".

[**AE**] Todo conjunto no vacío tiene una función de elección.

[**TIP**] Toda álgebra booleana contiene un ideal (propio) primo.

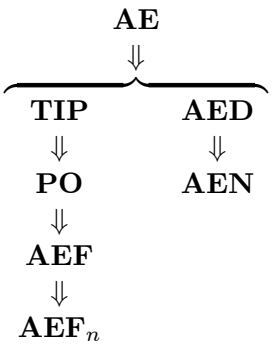
[**AED**] Si R es una relación en un conjunto no vacío X tal que para todo $x \in X$, existe $y \in X$ tal que xRy. Entonces existe una sucesión $\{x_n\}$ tal que $x_n R x_{n+1}$.

[**AEN**] Para cualquier familia numerable de conjuntos no vacíos $\{A_n\}_{n\in\mathbf{N}}$ existe una función $f : \mathbf{N} \to \bigcup_{n=0}^{\infty} A_n$ tal que $f(n) \in A_n$.

[**PO**] Todo conjunto puede ser linealmente ordenado.

[**AEF**] Para cualquier familia $\mathcal{F}$ de conjuntos finitos no vacíos existe una función $f : \mathcal{F} \to \bigcup \mathcal{F}$ tal que $f(F) \in F$.

[**AEF**$_n$] Cualquier familia $\mathcal{F}$ de conjuntos de n elementos, existe una función $f : \mathcal{F} \to \bigcup \mathcal{F}$ tal que $f(F) \in F$.



Ejercicios 8.6

1. Demuestre el Teorema 8.66.
2. Demuestre que el Principio de Ordenación **PO** implica el Axioma de Elección para conjuntos Finitos.
3. Demuestre que **AEF** implica **AEF**$_n$.

8.7 Matemáticas sin Elección.

Es muy interesante saber cómo son las matemáticas sin el Axioma de Elección. S. Feferman, como ya se mencionó, demostró que si no se acepta el Axioma de Elección se puede suponer que todos los ultrafiltros sobre los números naturales son principales. En esta sección daremos otros ejemplos que muestran lo grave que pueden ser las Matemáticas sin el Axioma de Elección. Para poder entenderlos, primero daremos una breve idea de lo que significa "un modelo". Esto lo haremos con base a un ejemplo.

Nosotros definimos los conjuntos ordenados como pares $(A, \leq)$ donde A es un conjunto y $\leq$ es una relación reflexiva, antisimétrica y transitiva en A. Equivalentemente, un conjunto ordenado es una estructura $(A, \leq)$, la cual satisface los siguientes axiomas:

Axioma de Reflexividad Para cada $a \in A$, $a \leq a$.

Axioma de Antisimetría. Si $a, b \in A$ y

$$a \leq b \qquad \text{y} \qquad b \leq a,$$

entonces $a = b$.

Axioma de Transitividad. Para cualesquiera $a, b, c \in A$, si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

Ahora podemos manifestar que los axiomas anteriores comprenden la *teoría axiomática del orden* y que los conjuntos ordenados son *modelos* de esta teoría axiomática. Nuestro análogo al Axioma de Elección en nuestra teoría del orden es el siguiente:

Axioma de Linealidad Para cualesquiera $a, b \in A$ o bien $a \leq b$ o $b \leq a$.

Si estamos interesados en saber cuándo el Axioma de Linealidad es consistente e independiente de los otros axiomas de la teoría del orden, necesitamos dar, por lo menos, dos modelos tal que en uno de ellos satisfaga el Axioma de Linealidad y en el otro no. Como posibles modelos tenemos los siguientes:

$$\left(\left(\{0, \{0\}\}\right), \in\right) \qquad \text{y} \qquad \left(\mathcal{P}(\{0, 1\}), \subseteq\right).$$

Esto nos lleva a concluir la independencia y consistencia del Axioma de Linealidad en nuestra teoría del orden.

Cuando se desea investigar fenómenos "extraños"; por ejemplo, que un subconjunto en un conjunto ordenado tenga dos distintos elementos maximales, necesitamos construir un modelo, es decir, un conjunto ordenado con tal propiedad. Un posible modelo es $(\mathcal{P}(\{0,1\}),\subseteq)$ con el subconjunto $X = \mathcal{P}(\{0,1\}) \setminus \{\{0,1\}\}$. En este modelo, $\{0\}$ y $\{1\}$ son distintos elementos - maximales de X. Por otra parte, podemos demostrar que dentro de la teoría del orden con el Axioma de Linealidad esto es imposible; así que la teoría del orden con linealidad es distinta de la teoría del orden.

Lo anterior es un ejemplo burdo de cómo se procedería para construir modelos para la Teoría de Conjuntos[3]. La técnica para construir tales modelos queda fuera de nuestro alcance, pero es posible tener una idea, al menos intuitiva, de lo que significan los siguientes enunciados.

1. Hay un modelo de **ZF** en el cual existe un conjunto infinito de números reales sin un subconjunto numerable.

2. Hay un modelo de **ZF** en el cual existe un conjunto de números reales y un punto de la clausura para el cual no existen sucesiones (en el conjunto) convergentes a dicho punto.

3. Hay un modelo de **ZF** tal que los números reales son unión a lo más numerable de conjuntos a lo más numerables.

4. Hay un modelo de **ZF** en el que existe un espacio vectorial sin base.

5. Hay un modelo de **ZF** en el cual todo conjunto de números reales es medible según Lebesgue.

[3]El Ejercicio 9.3.8 proporciona un modelo de **ZF** sin el Axioma de Infinitud.

9

Ordinales

9.1 Introducción

En el Capítulo 7 definimos el concepto de cardinalidad, pero la noción de cardinal en sí misma permanece velada excepto para los conjuntos finitos; esto es, hasta el momento no se tienen buenos representantes para conjuntos infinitos equipotentes, que desempeñen un papel análogo al de los números naturales para conjuntos finitos.

La idea central es generalizar el método conjuntista de la construcción de los números naturales, en el cual, un objeto es un número natural si es un conjunto transitivo, bien ordenado por la relación de pertenencia restringida y cualquier subconjunto no vacío tiene un elemento máximo con respecto a este orden. Así, n es un número natural, implica $n = \{0, 1, 2, \ldots, n-1\}$. Si denotamos

$$\omega = \{0, 1, 2, \ldots, n, n+1, \ldots\},$$

podemos pensar que ω es el primer "número" más grande que cualquier número natural. Llegado a este límite, la operación de sucesor puede ser empleada para generar "números" posteriores a ω del siguiente modo:

$$S(\omega) = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, n, \ldots, \omega\}$$

$$S(S(\omega)) = S(\omega) \cup \{S(\omega)\} = \{0, 1, 2, \ldots, \omega, S(\omega)\}$$

etc. Denotando a $S(\omega)$ como $\omega + 1$, tenemos:

$$S(\omega) = \omega + 1,$$

$$S(S(\omega)) = (\omega + 1) + 1 = \omega + 2,$$

etc.

Ahora tenemos una "sucesión" 0, 1, 2, ..., ω, $\omega+1$, $\omega+2$, $\omega+3$, ..., $\omega+n$, ..., para todo número natural $n \in \mathbf{N}$. Un "número mayor" a todo $\omega+n$ puede ser concebido como el conjunto de todos los números más pequeños

$$\omega \cdot 2 = \omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega + n, \ldots\}$$

y nuevamente para n tendríamos

$$\omega \cdot n = \{0, 1, 2, \ldots, \omega, \ldots, \omega \cdot 2, \ldots, \omega \cdot (n-1), \omega \cdot (n-1) + 1 \ldots\}$$

hasta llegar a

$$\omega \cdot \omega = \{0, 1, 2, \ldots, \omega, \ldots, \omega \cdot n, \ldots, \omega \cdot (n+1), \ldots\}.$$

Los conjuntos generados por este proceso poseen casi todas las propiedades requeridas por la definición de número natural. Son transitivos y están linealmente ordenados por $\in$, es decir, $x \in y$ implica $x \subseteq y$, y si $x, y \in z$ entonces

$$x < y \quad \text{si y sólo si} \quad x \in_z y$$

es un orden lineal.

Definición 9.1 Un conjunto x es un *ordinal* o *número ordinal* si y sólo si:
(a) x es transitivo,
(b) x es bien ordenado por $\in_x$.

Proposición 9.2 *Los números naturales son ordinales y hay un ordinal que no es un número natural, a saber,* ω.

El propósito de contar es el de comparar el tamaño de un conjunto con el de otro conocido. El método más familiar de contar los elementos de un conjunto es el de arreglarlos en un orden apropiado. La teoría de los números ordinales es una ingeniosa abstracción del método, pero se queda un tanto corta en la realización del propósito. El propio Cantor (su inventor) se dio cuenta que para conjuntos infinitos el orden no determina por completo la cardinalidad del conjunto. Esto no quiere decir que los números ordinales sean inútiles; simplemente sucede que su aplicación principal está en otra parte. Una muestra de su uso está en la topología como fuente de ejemplos y contraejemplos.

9.2 Números Ordinales

Fijándonos en la construcción de los números ordinales como apareció en la sección anterior, se puede observar que si α es un ordinal, entonces su sucesor también es un ordinal. Veamos que así es.

Proposición 9.3 *Si* α *es un número ordinal, entonces* $S(\alpha)$ *es también un número ordinal.*

DEMOSTRACIÓN:

$S(\alpha) = \alpha \cup \{\alpha\}$ es un conjunto transitivo. Más aún, $\alpha \cup \{\alpha\}$ es bien ordenado por $\in_{S(\alpha)}$, α es su elemento máximo y $\alpha \subseteq \alpha \cup \{\alpha\}$ es el segmento inicial determinado por α. Así, $S(\alpha)$ es un número ordinal. ■

Denotaremos al sucesor de α por $\alpha + 1$:

$$\alpha + 1 = S(\alpha) = \alpha \cup \{\alpha\}.$$

Sabemos que los números naturales y ω son ordinales. Una diferencia sustancial entre cualquier número natural $n \neq 0$ y ω es que n tiene un predecesor inmediato mientras que ω no lo tiene. Para distinguir a esta clase de ordinales hacemos la siguiente definición.

Definición 9.4 Un número ordinal α se llama *ordinal sucesor* si para algún ordinal β, $\alpha = \beta + 1$. En caso de que no exista un ordinal β del cual α sea sucesor, entonces a α se le llama *ordinal límite.*

Ejemplo 9.5 Los números naturales distintos de cero, $\omega + 1$, $\omega + 2$, $\omega \cdot 2 + 1$ son ordinales sucesores. 0, ω, $\omega \cdot 2$, $\omega \cdot \omega$ son ordinales límite.

Los siguientes tres lemas permitirán definir un orden en la clase de todos los ordinales que, como veremos después del siguiente teorema, no es un conjunto. Las demostraciones de los dos primeros lemas son idénticas a la de los Lemas 5.5 y 5.6.

Lema 9.6 *Cualquier elemento de un número ordinal es un número ordinal.*

Lema 9.7 *Si α es un número ordinal, entonces $\alpha \notin \alpha$. Si α y β son dos números ordinales entonces es falso que $(\alpha \in \beta \quad \wedge \quad \beta \in \alpha)$.*

Lema 9.8 *Si α y β son ordinales tales que $\alpha \subset \beta$, entonces $\alpha \in \beta$.*

DEMOSTRACIÓN:

Sea $\alpha \subset \beta$. Entonces $\beta \setminus \alpha$ es un subconjunto no vacío de β y, por tanto, tiene un elemento mínimo γ en el orden $\in_\beta$. Note que $\gamma \subseteq \alpha$; de no ser así, entonces cualquier $\delta \in \gamma \setminus \alpha$ sería un elemento de $\beta \setminus \alpha$ menor que γ (por la transitividad de β), lo cual es imposible.

Para completar la demostración, mostremos que $\alpha \subseteq \gamma$ (con esto $\alpha = \gamma \in \beta$). Sea $\delta \in \alpha$. Si ocurriera $\delta \notin \gamma$, entonces o bien $\gamma \in \delta$ o $\delta = \gamma$ (porque β está linealmente ordenado por $\in_\beta$ y $\gamma, \delta \in \beta$). Pero esto implica que $\gamma \in \alpha$, ya que α es transitivo; contradiciendo la elección de $\gamma \in \beta \setminus \alpha$. ■

Definición 9.9 Para ordinales α y β definimos $\alpha < \beta$ si y sólo si $\alpha \in \beta$.

Obsérvese que esté orden extiende al orden que se definió para los números naturales. El siguiente teorema muestra que $\leq$ es de hecho un buen orden.

Teorema 9.10 *Sean α, β, y γ números ordinales.*

(a) Si $\alpha < \beta$ y $\beta < \gamma$, entonces $\alpha < \gamma$.

(b) $\alpha < \beta$ y $\beta < \alpha$ no pueden cumplirse simultáneamente.

(c) Una de las relaciones $\alpha < \beta$, $\alpha = \beta$ o $\beta < \alpha$ se satisface.

(d) Sea X un conjunto de números ordinales entonces $(X, \leq)$ es un conjunto bien ordenado.

(e) Para todo conjunto de ordinales X hay un ordinal α tal que $\alpha \notin X$. (En otras palabras el conjunto de todos los números ordinales no existe.)

Demostración:

(a) Si $\alpha \in \beta$ y $\beta \in \gamma$, entonces $\alpha \in \gamma$ puesto que γ es transitivo.

(b) Es una consecuencia del Lema 9.7.

(c) Si α y β son ordinales, entonces $\alpha \cap \beta$ es un número ordinal y $\alpha \cap \beta \subseteq \alpha$ y $\alpha \cap \beta \subseteq \beta$. Si $\alpha \cap \beta = \alpha$, entonces $\alpha \subseteq \beta$, lo cual implica que $\alpha \in \beta$ o $\alpha = \beta$. Similarmente, si $\alpha \cap \beta = \beta$, entonces $\beta \in \alpha$ o $\beta = \alpha$. El único caso restante es $\alpha \cap \beta \subset \alpha$ y $\alpha \cap \beta \subset \beta$, que no puede ocurrir puesto que entonces obtendríamos $\alpha \cap \beta \in \alpha$ y $\alpha \cap \beta \in \beta$, y así $\alpha \cap \beta \in \alpha \cap \beta$; contradiciendo el Lema 9.7.

(d) Por el Lema 9.7, $<$ es asimétrica en X, por (a) es transitiva y por el Teorema 4.103(b) $(X, \leq)$ es un conjunto ordenado. Veamos que $(X, \leq)$ es bien ordenado. Sea $A \subseteq X$ no vacío, tomando $\alpha \in A$ y considerando $\alpha \cap A$ tenemos:

Si $\alpha \cap A = \emptyset$, entonces α es el primer elemento de A.

Si $\alpha \cap A \neq \emptyset$, $\alpha \cap A \subseteq \alpha$ tiene un primer elemento β con el orden $\in_\alpha$, entonces β es el primer elemento de A con el orden $\leq$.

(e) Sea X un conjunto de números ordinales. Puesto que todos los elementos de X son conjuntos transitivos, $\bigcup X$ también es un conjunto transitivo (ver Ejercicio 5.1.7). Por la parte (d) de este teorema, se tiene que $\in$ es un buen orden para $\bigcup X$. Consecuentemente, $\bigcup X$ es un número ordinal. Ahora, sea $\alpha = S(\bigcup X)$. α es un ordinal y $\alpha \notin X$ ya que si $\alpha \in X$ entonces $\alpha \subseteq \bigcup X$ por el Lema 9.8; lo cual implica que $\alpha = \bigcup X$ o $\alpha \in \bigcup X$ y en ambos casos $\alpha \in S(\bigcup X) = \alpha$, que es una contradicción. ■

Definición 9.11 El número ordinal $\bigcup X$ usado en la demostración de la parte (e) del Teorema 9.10 es llamado *supremo* de X y se denota por $\sup X$.

La definición anterior se justifica observando que $\bigcup X$ es el mínimo ordinal mayor o igual que todos los elementos de X. En efecto, $\alpha \in X$ implica $\alpha \subseteq$

$\bigcup X$, así $\alpha \leq \bigcup X$, y si $\alpha \leq \gamma$ para todo $\alpha \in X$, entonces $\alpha \subseteq \gamma$ para todo $\alpha \in X$, luego $\bigcup X \subseteq \gamma$, es decir, $\bigcup X \leq \gamma$.

Si el conjunto X tiene un elemento máximo β en el orden $\leq$, entonces $\sup X = \beta$. De otro modo $\sup X > \gamma$ para todo $\gamma \in X$ (y éste es el mínimo de tales ordinales). También es conveniente observar que todo conjunto de ordinales tiene un supremo (en el orden $\leq$).

Si denotamos por **Ord** a la clase de todos los números ordinales (que, como se demostró, no es un conjunto), entonces según nuestro acuerdo de la Sección 4.6, podemos decir que **Ord** es una clase bien ordenada con la propiedad de la máxima cota superior (ver Ejercicio 4.5.22).

El último teorema de esta sección asegura el hecho de que los ordinales son una generalización de los números naturales.

Teorema 9.12 *Los números naturales son exactamente los números ordinales finitos.*

Demostración:

Sabemos que todo número natural es un número ordinal, y de hecho, cualquier número natural es un conjunto finito. Así, únicamente probaremos que todo ordinal que no es un número natural es un conjunto infinito.

Si α es un número ordinal y $\alpha \notin \mathbf{N}$, entonces por el Teorema 9.10 se debe tener que $\omega \leq \alpha$ (puesto que $\alpha \not< \omega$). Dado que α es transitivo, $\omega \subseteq \alpha$. Por lo anterior, α tiene un subconjunto infinito; con lo cual se concluye que es infinito. ■

Todo número ordinal es un conjunto bien ordenado bajo el ordenamiento $\in$. Si α y β son distintos ordinales, entonces ellos no son isomorfos como conjuntos bien ordenados; puesto que uno es un segmento inicial del otro (Teorema 4.138). Posteriormente probaremos que cualquier conjunto bien ordenado es isomorfo a un número ordinal. Sin embargo, esto requiere la introducción de otro axioma, y esto se hace en la siguiente sección.

Un comentario final: el Lema 9.6 establece que cada número ordinal α se puede expresar como

$$\alpha = \{\beta : \beta \ \in \mathbf{Ord} \text{ y } \beta < \alpha\}.$$

Si nosotros vemos a α como un conjunto de ordinales, entonces si α es un ordinal sucesor, digamos $\beta + 1$, α tiene un elemento máximo, a saber, β. Si α es un ordinal límite, entonces α no tiene un elemento máximo y $\alpha = \sup\{\beta : \beta < \alpha\}$.

Note también que 0 es un ordinal límite y que $\sup \emptyset = 0$.

Ejercicios 9.2

1. Muestre que un ordinal α es un número natural si y sólo si todo subconjunto no vacío de α tiene un elemento máximo.

2. Demuestre que si un conjunto de ordinales X no tiene un elemento máximo, entonces $\sup X$ es un ordinal límite.

3. Pruebe que si $x \subseteq \mathbf{Ord}$, entonces $x \in \mathbf{Ord}$ si y sólo si x es transitivo.

4. Sea α es un ordinal límite y sea $\beta \subseteq \alpha$. Pruebe que si para cada $\gamma \in \alpha$ existe $\delta \in \beta$ tal que $\gamma \in \delta$, entonces $\alpha = \bigcup \beta$.

9.3 El Axioma de Reemplazo

Como indicamos en la sección precedente, los conjuntos bien ordenados pueden ser representados por los números ordinales, es decir, cualquier conjunto bien ordenado es isomorfo a un único número ordinal. Sin embargo, como también afirmamos, requerimos de otro axioma. Veamos por qué es necesario.

Para construir una sucesión

$$(\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots)$$

podemos definir

$$a_0 = \emptyset,$$

$$a_{n+1} = \{a_n\}, \quad \text{para cada } n \in \mathbf{N},$$

siguiendo el patrón general de definiciones recursivas. La dificultad aquí es que para aplicar el Teorema de Recursión necesitamos un conjunto A, *dado de antemano*, tal que $g : \mathbf{N} \times A \to A$ definida por $g(n, x) = \{x\}$ pueda ser usada para calcular el $(n + 1)$-ésimo término de la sucesión a partir del n-ésimo término. Pero no es enteramente obvio cómo probar desde nuestros axiomas que exista un conjunto A tal que

$$\emptyset \in A, \quad \{\emptyset\} \in A, \quad \{\{\emptyset\}\} \in A, \quad \{\{\{\emptyset\}\}\} \in A, \ldots$$

Parece que la definición de A mismo requiere de recursión.

Consideremos otro ejemplo. En el Capítulo 5, postulamos la existencia de ω; a partir de éste, los conjuntos $\omega + 1 = \omega \cup \{\omega\}$, $\omega + 2 = (\omega + 1) \cup \{\omega + 1\}$, etc., pueden obtenerse fácilmente por usos repetidos de unión y par no ordenado. En la introducción de este capítulo "definimos" $\omega + \omega$ como el conjunto de

todos los $\omega + n$ para todo $n \in \omega$ y pasamos por alto postular la existencia de $\omega + \omega$ como conjunto. La existencia de $\omega + \omega$ no puede ser demostrada a partir de los axiomas anteriormente aceptados. Sabemos que a cada $n \in \omega$, le corresponde un único conjunto $\omega + n$, pero no tenemos algún axioma que nos diga que podemos coleccionar a todo $\omega + n$ en un conjunto.

Axioma 10 (Esquema de Reemplazo) *Sea* $\mathbf{P}(x, y)$ *una propiedad tal que para todo* x *existe un único* y *para el cual* $\mathbf{P}(x, y)$ *se satisface.*

Para todo conjunto A*, existe un conjunto* B *tal que, para todo* $x \in A$*, existe* $y \in B$ *para el cual* $\mathbf{P}(x, y)$ *se satisface.*

Se espera que los siguientes comentarios den motivaciones adicionales a la introducción del Axioma Esquema de Reemplazo.

Sea $\mathbf{F}$ la (clase) función (en el sentido de la Sección 4.6) definida por la propiedad $\mathbf{P}(x, y)$; esto es, $\mathbf{F}(x)$ denota al único y para el cual $\mathbf{P}(x, y)$ se satisface. El correspondiente Axioma de Reemplazo puede usarse como sigue:

Para todo conjunto A hay un conjunto B tal que para todo

$$x \in A, \ \ \mathbf{F}(x) \in B.$$

De hecho, B puede también contener elementos que no sean de la forma $\mathbf{F}(x)$ con $x \in A$; sin embargo, una aplicación del Axioma Esquema de Comprensión muestra que

$$\begin{aligned} \{y \in B : \exists\, x \in A, \ y = \mathbf{F}(x)\} \ &= \{y \in B : \exists x \in A, \ \mathbf{P}(x, y)\} \\ &= \{y : \exists x \in A, \ \mathbf{P}(x, y) \ \} \end{aligned}$$

existe. Llamamos a este conjunto la *imagen* de A por $\mathbf{F}$ y denotamos éste por $\{\mathbf{F}(x) : x \in A\}$ o simplemente $\mathbf{F}(A)$.

Una justificación intuitiva para el Axioma Esquema de Reemplazo puede darse comparándolo con el Axioma Esquema de Comprensión. Este último nos concede ir a través de los elementos de A, verificar para cada $x \in A$ si x tiene o no tiene la propiedad $\mathbf{P}(x)$, y coleccionar a aquellos x que tienen la propiedad en un conjunto. De manera enteramente análoga, el Axioma Esquema de Reemplazo permite ir a través de los elementos de A, y tomar para cada $x \in A$ el correspondiente y que tiene la propiedad $\mathbf{P}(x, y)$ y coleccionar a tales y en un conjunto. Intuitivamente es obvio que el conjunto $\mathbf{F}(A)$ "no es más grande" que el conjunto A. En contraste, todos los ejemplos conocidos de "conjuntos paradójicos" son "grandes", digamos del orden de la clase de todos los conjuntos.

Sea **F** nuevamente una (clase) función definida por **P**. El Axioma de Reemplazo implica que la función **F** sobre los elementos de A puede ser representada, o bien "reemplazada", por una función legítima, es decir, un conjunto de pares ordenados. Precisamente,

> Para cualquier conjunto A, hay una función f tal que $dom\, f = A$ y $f(x) = \mathbf{F}(x)$ para todo $x \in A$.

Simplemente, sea $f = \{(x, y) \in A \times B : \mathbf{P}(x, y)\}$, donde B es el conjunto provisto por el Axioma de Reemplazo.

Zermelo, en su axiomatización de 1908, no dio el Axioma de Reemplazo y sólo usaba el Axioma Esquema de Comprensión. El Axioma de Reemplazo fue propuesto independientemente por Mirimanoff [M_2] en 1917, Skolem [S_6] en 1919 y Fraenkel [F_1] en 1922; sin embargo, el artículo de Fraenkel fue más influyente y por esta razón el axioma usualmente es acreditado a Fraenkel. Von Neumann mostró que por medio de la noción de *clase* se puede reemplazar el Axioma Esquema de Reemplazo por una única proposición de manera similar a como se hace con el Axioma Esquema de Comprensión (véase Apéndice B).

Ahora enunciaremos formalmente y demostraremos el resultado que anunciamos al inicio de esta sección.

Teorema 9.13 *Todo conjunto bien ordenado es isomorfo a un único número ordinal.*

Demostración:

Sea $(W, \preceq)$ un conjunto bien ordenado. Dado que dos ordinales isomorfos son iguales, bastará probar la existencia de un ordinal que sea isomorfo a $(W, \preceq)$. Para cada $x \in W$, sea W_x el segmento inicial de W determinado por x y sea A el conjunto de todos los $x \in W$ tales que el conjunto bien ordenado $(W_x, \preceq)$ es isomorfo a algún ordinal. Entonces, para todo $x \in A$, por la observación anterior sobre ordinales isomorfos, sólo un ordinal, digamos α_x, es isomorfo a $(W_x, \preceq)$.

Sea $\mathbf{P}(x, y)$ la propiedad: "O bien $x \in W$ y y es el único ordinal isomorfo a $(W_x, \preceq)$, o $x \notin W$ y $y = \emptyset$". Aplicando el Axioma Esquema de Reemplazo, existe una función f de A en algún conjunto de ordinales, definida por:

$$f = \{(x, \alpha_x) : x \in A,\ \alpha_x \text{ isomorfo a } (W_x, \preceq)\}.$$

Sea α un ordinal tal que $\alpha \notin f(A)$.

Para completar la demostración usaremos el Teorema 4.138. $(\alpha, \leq)$ es un conjunto bien ordenado, entonces o $(\alpha, \leq)$ es isomorfo a $(W, \preceq)$, y en tal caso

terminaríamos la prueba, o bien $(W, \preceq)$ es isomorfo a un segmento inicial de α, en tal caso este segmento inicial de α es un número ordinal. La última posibilidad es que $(\alpha, \leq)$ sea isomorfo a un segmento inicial de W, pero esto implicaría $\alpha \in f(A)$ contradiciendo la elección de α. ■

Definición 9.14 Si $(W, \preceq)$ es un conjunto bien ordenado, entonces el *tipo de orden de* $(W, \leq)$ es el único número ordinal isomorfo a W. $\|(W, \preceq)\|$ denotará el tipo de orden de $(W, \preceq)$.

Corolario 9.15 *Sean* $(W_1, \preceq_1)$ *y* $(W_2, \preceq_2)$ *dos conjuntos bien ordenados. Entonces* $(W_1, \preceq_1)$ *es isomorfo a* $(W_2, \preceq_2)$ *si y sólo si*

$$\|(W_1, \preceq_1)\| = \|(W_2, \preceq_2)\|.$$

Teorema 9.16 *Un conjunto* W *puede ser bien ordenado si y sólo si es equipotente a un número ordinal.*

Demostración:

Sea $\preceq$ un buen orden para W. El isomorfismo entre $(W, \preceq)$ y $\|(W, \preceq)\|$ es una biyección entre W y $\|(W, \preceq)\|$.

Recíprocamente, si $f : W \to \alpha$ es una biyección, entonces para $x, y \in W$,

$$x \preceq y \quad \text{si y sólo si} \quad f(x) \leq f(y)$$

es un buen orden para W. ■

Corolario 9.17 *El Axioma de Elección es equivalente a que todo conjunto es equipotente a algún número ordinal.*

Finalizamos esta sección con una generalización del Teorema de Recursión del Capítulo 5, la cual resuelve la existencia de una sucesión $(\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots)$.

Teorema 9.18 (de Recursión Generalizada) *Sea* $\mathbf{G}$ *una (clase) función. Para cualquier conjunto* a *existe una única sucesión* $(a_n)_{n=0}^{\infty}$ *tal que*

(a) $a_0 = a$,

(b) $a_{n+1} = \mathbf{G}(a_n, n)$ *para todo* $n \in \mathbf{N}$.

Probaremos este Teorema de Recursión Generalizada, como también el Teorema de Recursión Transfinita más general, en la siguiente sección.

Ejercicios 9.3

1. Demuestre lo siguiente: Sea $\mathbf{P}(x, y)$ una propiedad tal que para todo x hay a lo más un y tal que $\mathbf{P}(x, y)$ se satisface. Entonces para cualquier conjunto A, existe un conjunto B tal que, para todo $x \in A$ si $\mathbf{P}(x, y)$ se satisface para algún y, entonces $\mathbf{P}(x, y)$ se satisface para algún $y \in B$.

2. Use el Teorema de Recursión Generalizada para probar la existencia de los siguientes conjuntos:

   (a) El conjunto $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots\}$.

   (b) El conjunto $\{\mathbf{N}, \mathcal{P}(\mathbf{N}), \mathcal{P}(\mathcal{P}(\mathbf{N})), \ldots\}$.

   (c) El conjunto $\omega + \omega = \omega \cup \{\omega, \omega + 1, \omega + 2, \omega + 3, \ldots\}$.

3. (a) Pruebe que el tipo de orden del conjunto $\omega \times 2$, con el orden lexicográfico horizontal (ver Ejemplo 4.112 y Ejercicio 4.5.29) es $\omega \cdot 2 = \omega + \omega$, y con el orden lexicográfico vertical es ω.

   (b) Pruebe que el tipo de orden del conjunto $2 \times \omega$, con el orden lexicográfico horizontal es ω, y con el orden lexicográfico vertical es $\omega \cdot 2 = \omega + \omega$.

4. Pruebe que si $(W, \leq)$ es un conjunto bien ordenado con

$$\|(W, \leq)\| = \alpha,$$

   entonces α es un ordinal límite si y sólo si W no tiene elemento máximo.

5. Use el Teorema de Recursión Generalizada para definir:

$$\begin{aligned} &V_0 = \emptyset, \\ &V_{n+1} = \mathcal{P}(V_n), \quad n \in \omega, \\ &V_\omega = \textstyle\bigcup_{n \in \omega} V_n. \end{aligned}$$

6. Demuestre que

   (a) Cualquier $x \in V_n$ es finito.

   (b) V_ω es transitivo.

   (c) V_ω es un conjunto inductivo. (Los elementos de V_ω se llaman conjuntos *hereditariamente finitos*.)

7. Demuestre que

(a) Si $x, y \in V_\omega$, entonces $\{x, y\} \in V_\omega$.

(b) Si $X \in V_\omega$, entonces $\bigcup X \in V_\omega$ y $\mathcal{P}(X) \in V_\omega$.

(c) Si $A \in V_\omega$ y f es una función en A tal que $f(x) \in V_\omega$ para cada $x \in A$, entonces $f(A) \in V_\omega$.

(d) Si X es un subconjunto finito de V_ω, entonces $X \in V_\omega$.

8. Demuestre que V_ω es un modelo para **ZF** sin el Axioma de Infinitud, donde $\in$ es la pertenencia usual de **ZF** y el término conjunto es el mismo que el de **ZF**, es decir, tomando como conjuntos a los objetos de V_ω se pueden verificar los axiomas del 1 al 10 a excepción del 8 y 9.

9.4 Inducción y Recursión Transfinita

El Principio de Inducción y el Teorema de Recursión son las principales herramientas para demostrar teoremas acerca de números naturales y para construir funciones con dominio **N**. En esta sección, mostraremos cómo estos resultados se generalizan a los números ordinales.

Teorema 9.19 (Principio de Inducción Transfinita) *Sea* $\mathbf{P}(x)$ *una propiedad (posiblemente con parámetros). Supongamos que, para todos los números ordinales* α

$$\textit{si } \mathbf{P}(\beta) \textit{ se cumple para todo } \beta < \alpha, \textit{ entonces } \mathbf{P}(\alpha) \textit{ se cumple.} \tag{9.4.1}$$

Entonces $\mathbf{P}(\alpha)$ *se cumple para todos los ordinales* α.

Demostración:

Supóngase que $\mathbf{P}(\alpha)$ falla para algún ordinal α. Sea

$$A = \{\beta \leq \alpha : \mathbf{P}(\beta) \text{ falla}\},$$

entonces $A \neq \emptyset$ y así tiene un primer elemento β_0.

$\mathbf{P}(\beta_0)$ falla, pero $\mathbf{P}(\beta)$ se cumple para todo $\beta < \beta_0$, lo cual contradice la hipótesis (9.4.1). ■

Algunas veces es conveniente usar el Principio de Inducción Transfinita en una forma que se parezca más a la formulación usual del Principio de Inducción para **N**. Al hacer esto, debemos tratar a los ordinales sucesores y a los ordinales límite por separado.

Teorema 9.20 (Segunda Versión del Principio de Inducción Transfinita) *Sea* $\mathbf{P}(x)$ *una propiedad (posiblemente con parámetros). Supongamos que:*

(a) $\mathbf{P}(0)$ *se cumple,*

(b) $\mathbf{P}(\alpha)$ *implica* $\mathbf{P}(\alpha+1)$ *para todos los ordinales* α*,*

(c) Para todo ordinal límite $\alpha \neq 0$*, si* $\mathbf{P}(\beta)$ *se cumple para cada* $\beta < \alpha$*, entonces* $\mathbf{P}(\alpha)$ *se cumple.*

Entonces $\mathbf{P}(\alpha)$ *se cumple para todos los ordinales* α*.*

Demostración:

Es suficiente mostrar que *(a)*, *(b)* y *(c)* implican (9.4.1). Sea α un ordinal tal que $\mathbf{P}(\beta)$ se cumple para todo $\beta < \alpha$. Si $\alpha = 0$, entonces $\mathbf{P}(\alpha)$ se cumple por *(a)*. Si α es sucesor, es decir, si existe β tal que $\alpha = \beta + 1$, sabemos que $\mathbf{P}(\beta)$ se cumple y así $\mathbf{P}(\alpha)$ se cumple por *(b)*. Si α es un ordinal límite distinto de 0, entonces $\mathbf{P}(\alpha)$ se cumple por *(c)*. ■

En la Sección 5.3 el Teorema de Recursión fue derivado del Principio de Inducción. Se demostró que si una función está definida en 0, y siempre que la función esté definida en n, su valor en $n+1$ puede determinarse, entonces existe una función cuyo dominio es $\mathbf{N}$. Alternativamente, siempre que una función esté definida para todos los naturales menores que n, su valor en n puede determinarse, entonces existe una función definida sobre $\mathbf{N}$. Ahora procederemos a generalizar el Teorema de Recursión a **Ord** usando el Principio de Inducción Transfinita. Funciones cuyo dominio es un ordinal α se llaman *sucesiones transfinitas de longitud* α.

Teorema 9.21 *Sea* Ω *un número ordinal, sea* A *un conjunto y sea* $S = \bigcup_{\alpha<\Omega} A^\alpha$ *el conjunto de todas las sucesiones transfinitas de elementos en* A *de longitud menor que* Ω*. Sea* $g : S \to A$ *una función. Entonces existe una única función* $f : \Omega \to A$ *tal que*

$$f(\alpha) = g(f\mid_\alpha) \qquad \text{para todo } \alpha < \Omega.$$

El lector puede probar este teorema de manera enteramente análoga a la prueba del Teorema de Recursión del Capítulo 5. No entraremos en los detalles puesto que el Teorema 9.21 se sigue desde un teorema posterior de recursión transfinita más general.

Si ϑ es un ordinal y si f es una sucesión transfinita de longitud ϑ. Usaremos la notación

$$f = (a_\alpha)_{\alpha<\vartheta}.$$

El Teorema 9.21 asegura que si g es una función en el conjunto de todas las sucesiones transfinitas de longitud menor que Ω con valores en A, entonces hay una sucesión transfinita $(a_\alpha)_{\alpha<\Omega}$ tal que para todo $\alpha < \Omega$,

$$a_\alpha = g\left((a_\xi)_{\xi<\alpha}\right).$$

Teorema 9.22 (de Recursión Transfinita) *Si* $\mathbf{G}$ *una (clase) función, entonces la propiedad* $\mathbf{P}$ *formulada en (9.4.2) define una (clase) función* $\mathbf{F}$ *tal que* $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F}\mid_\alpha)$ *para todos los ordinales* α.

Demostración:

Llamaremos a t *cálculo de longitud* α *basado en* $\mathbf{G}$, si t es una función, $dom\, t = \alpha + 1$ y para todo $\beta \leq \alpha$, $t(\beta) = \mathbf{G}(t\mid_\beta)$.

Sea $\mathbf{P}(x, y)$ la propiedad

$$\left.\begin{array}{r} x \text{ es un número ordinal y } y = t(x) \text{ para algún} \\ \text{cálculo } t \text{ de longitud } x \text{ basado en } \mathbf{G}, \\ \text{o } x \text{ no es un número ordinal y } y = \emptyset. \end{array}\right\} \tag{9.4.2}$$

Probaremos primero que $\mathbf{P}$ define una (clase) función.

Tenemos que demostrar que para cada x hay un único y tal que $\mathbf{P}(x, y)$. Esto es obvio si x no es un número ordinal. Para mostrarlo para los ordinales, es suficiente probar por inducción transfinita que para cualquier ordinal α existe un único cálculo de longitud α.

Hagamos la suposición inductiva de que para cada $\beta < \alpha$ existe un único cálculo de longitud β, y demostremos la existencia y unicidad de un cálculo de longitud α.

Existencia. De acuerdo al Axioma Esquema de Reemplazo aplicado a la propiedad "y es un cálculo de longitud x o $x \notin \alpha,\ y = \emptyset$" y al conjunto α, existe un conjunto

$$T = \{t : t \text{ es un cálculo de longitud } \beta \text{ para algún } \beta < \alpha\}.$$

Más aún, la suposición inductiva implica que para cada $\beta < \alpha$ existe un único $t \in T$ tal que la longitud de t es β.

T es un sistema compatible de funciones; sea $\overline{t} = \bigcup T$. Finalmente, sea $\tau = \overline{t} \cup \left\{(\alpha, \mathbf{G}(\overline{t}))\right\}$. Probaremos que τ es un cálculo de longitud α.

Afirmación: τ es una función y $dom\, \tau = \alpha + 1$.

Se tiene que $dom\, \overline{t} = \bigcup_{t\in T} dom\, t = \bigcup_{\beta<\alpha}(\beta + 1) = \alpha$; consecuentemente, $dom\, \tau = dom\, \overline{t} \cup \{\alpha\} = \alpha + 1$. Como $\alpha \notin dom\, \overline{t}$, es suficiente mostrar que $\overline{t}$ es una función. Esto se sigue del hecho de que T es un sistema compatible de

funciones. En efecto, sean $t_1, t_2 \in T$ arbitrarios, y sean $dom\, t_1 = \beta_1$, $dom\, t_2 = \beta_2$. Supongamos, sin pérdida de generalidad, que $\beta_1 \leq \beta_2$; entonces $\beta_1 \subseteq \beta_2$, y es suficiente probar que $t_1(\gamma) = t_2(\gamma)$ para todo $\gamma < \beta_1$. Usaremos inducción transfinita. Supongamos que $\gamma < \beta_1$ y $t_1(\delta) = t_2(\delta)$ para todo $\delta < \gamma$. Entonces $t_1 \mid_\gamma = t_2 \mid_\gamma$, y tenemos que

$$t_1(\gamma) = \mathbf{G}(t_1 \mid_\gamma) = \mathbf{G}(t_2 \mid_\gamma) = t_2(\gamma).$$

Lo cual nos lleva a concluir que $t_1(\gamma) = t_2(\gamma)$ para todo $\gamma < \beta_1$. Esto completa la prueba de la afirmación.

Afirmación: $\tau(\beta) = \mathbf{G}(\tau \mid_\beta)$ para todo $\beta \leq \alpha$.

Esto es claro si $\beta = \alpha$, pues $\tau(\alpha) = \mathbf{G}(\bar{t}) = \mathbf{G}(\tau \mid_\alpha)$. Si $\beta < \alpha$, tomemos $t \in T$ tal que $\beta \in dom\, t$. Tenemos entonces que:

$$\tau(\beta) = t(\beta) = \mathbf{G}(t \mid_\beta) = \mathbf{G}(\tau \mid_\beta)$$

puesto que t es un cálculo y $t \subseteq \tau$.

Las dos afirmaciones anteriores juntas demuestran que τ es un cálculo de longitud α.

Unicidad. Sea σ otro cálculo de longitud α. Probaremos que $\tau = \sigma$. Como τ y σ son funciones y $dom\, \tau = \alpha + 1 = dom\, \sigma$, es suficiente probar por inducción transfinita que $\tau(\gamma) = \sigma(\gamma)$ para todo $\gamma \leq \alpha$.

Supongamos que $\tau(\delta) = \sigma(\delta)$ para todo $\delta < \gamma$. Entonces $\tau(\gamma) = \mathbf{G}(\tau \mid_\gamma) = \mathbf{G}(\sigma \mid_\gamma) = \sigma(\gamma)$. Por tanto, $\tau(\gamma) = \sigma(\gamma)$ para todo $\gamma \leq \alpha$, así $\tau = \sigma$.

Lo anterior concluye la demostración de que $\mathbf{P}$ define una (clase) función $\mathbf{F}$. Note que para cualquier cálculo t, $\mathbf{F} \mid_{dom\, t} = t$. Esto es porque para cualquier $\beta \in dom\, t$, $t_\beta = t \mid_{\beta+1}$ es obviamente un cálculo de longitud β, y así, por definición de $\mathbf{F}$, $\mathbf{F}(\beta) = t_\beta(\beta) = t(\beta)$.

Para probar que $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \mid_\alpha)$ para todo α, sea t el único cálculo de longitud α, tenemos entonces que:

$$\mathbf{F}(\alpha) = t(\alpha) = \mathbf{G}(t \mid_\alpha) = \mathbf{G}(\mathbf{F} \mid_\alpha). \quad \blacksquare$$

Necesitamos nuevamente una versión paramétrica del Teorema de Recursión Transfinita. Si $\mathbf{F}(z, x)$ es una (clase) función de dos variables, escribiremos $\mathbf{F}_z(x)$ en lugar de $\mathbf{F}(z, x)$. Note que para z fijo, $\mathbf{F}_z$ es una (clase) función en una variable. Si $\mathbf{F}$ es definida por $\mathbf{H}(z, x, y)$, las notaciones $\mathbf{F}_z(A)$ y $\mathbf{F}_z \mid_A$ tienen los significados siguientes:

$$\mathbf{F}_z(A) = \{y : \mathbf{H}(z, x, y) \text{ para algún } x \in A\};$$

$$\mathbf{F}_z \mid_A = \{(x, y) : \mathbf{H}(z, x, y) \text{ para algún } x \in A\}.$$

Ahora podemos mostrar la versión paramétrica del Teorema de Recursión Transfinita.

Teorema 9.23 (Recursión Transfinita Paramétrica) *Sea* $\mathbf{G}$ *una (clase) función de dos variables. La propiedad* $\mathbf{H}$ *formulada en (9.4.3) define una (clase) función* $\mathbf{F}$ *tal que* $\mathbf{F}(z,\alpha) = \mathbf{G}(z, \mathbf{F}_z \mid_\alpha)$ *para todos los ordinales* α *y todo conjunto* z.

Demostración:

Llamamos a t un *cálculo de longitud* α *basado en* $\mathbf{G}$ y z si t es una función, $dom\, t = \alpha + 1$ y para todo $\beta \leq \alpha$, $t(\beta) = \mathbf{G}(z, t \mid_\beta)$.

Sea $\mathbf{H}$ la propiedad

$$\left.\begin{array}{r} x \text{ es un número ordinal y } y = t(x) \text{ para algún} \\ \text{cálculo } t \text{ de longitud } x \text{ basado en } \mathbf{G} \text{ y } z \\ \text{o } x \text{ no es un número ordinal y } y = \emptyset. \end{array}\right\} \tag{9.4.3}$$

Entonces z recorre como un parámetro a través del resto de la demostración del Teorema de Recursión Transfinita. ■

Ejercicios 9.4

1. Demuestre el Teorema de Recursión Generalizada.

2. Demuestre el Teorema 9.21.

3. Demuestre la siguiente versión que generaliza al Teorema de Recursión Transfinita (Teorema de Doble Recursión): Sea $\mathbf{G}$ una (clase) función de dos variables. Entonces existe una (clase) función $\mathbf{F}$ tal que $\mathbf{F}(\alpha,\beta) = \mathbf{G}(\mathbf{F} \mid_{\alpha\times\beta})$ para todos los ordinales α y β. (Sugerencia: los cálculos son ahora funciones con dominio $(\alpha+1)\times(\beta+1)$.)

4. Usando el Teorema de Recursión Transfinita Paramétrica muestre que hay una (clase) función tal que:

   (a) $\mathbf{F}(x,1) = 0$ para todo x.

   (b) $\mathbf{F}(x, n+1) = 0$ si y sólo si existen $y,\ z$ tal que $x = (y,z)$ y $\mathbf{F}(y,n) = 0$.

5. Complete la demostración del Teorema de Recursión Transfinita Paramétrica.

6. Demuestre que hay una cantidad no numerable de buenos órdenes en $\mathbf{N}$ de tal modo que dos diferentes de tales órdenes no son isomorfos.

9.5 Aritmética Ordinal

Ahora usaremos el Teorema de Recursión Transfinita mencionado en la sección anterior para definir suma, multiplicación y exponenciación de números ordinales. Estas definiciones son amplias generalizaciones de las correspondientes para números naturales.

Es necesario distinguir entre ordinales sucesores y ordinales límite en nuestra construcción. También conviene reformular el Teorema de Recursión con esta distinción en mente.

Teorema 9.24 *Sean* $\mathbf{G}_1$, $\mathbf{G}_2$ *y* $\mathbf{G}_3$ *(clase) funciones, y sea* $\mathbf{G}$ *la (clase) función que define la propiedad definida en (9.5.1). Entonces la propiedad* $\mathbf{P}$ *formulada en (9.4.2) (basada en* $\mathbf{G}$*) define una función* $\mathbf{F}$ *tal que:*

(a) $\mathbf{F}(0) = \mathbf{G}_1(\emptyset)$,

(b) $\mathbf{F}(\alpha + 1) = \mathbf{G}_2(\mathbf{F}(\alpha))$ *para todo* α,

(c) $\mathbf{F}(\alpha) = \mathbf{G}_3(\mathbf{F} \mid_\alpha)$ *para todo ordinal límite* $\alpha \neq 0$.

DEMOSTRACIÓN:

Defina una operación $\mathbf{G}$ por $\mathbf{G}(x) = y$ si y sólo si

$$\left.\begin{array}{lll} \text{o bien} & \text{(i)} & x = \emptyset, \;\; y = \mathbf{G}_1(\emptyset) \\ \text{o} & \text{(ii)} & \left\{\begin{array}{r} x \text{ es una función, } \; dom\, x = \alpha + 1 \\ \text{para algún ordinal } \alpha \neq 0, \\ y = \mathbf{G}_2(x(\alpha)) \end{array}\right. \\ \text{o} & \text{(iii)} & \left\{\begin{array}{r} x \text{ es una función, } \; dom\, x = \alpha \\ \text{para algún ordinal límite} \\ \alpha \neq 0, \;\; y = \mathbf{G}_3(x) \end{array}\right. \\ \text{o} & \text{(iv)} & x \text{ no es nada de lo anterior y } y = \emptyset \end{array}\right\} \tag{9.5.1}$$

Sea $\mathbf{P}$ la propiedad formulada en (9.4.2) de la demostración del Teorema de Recursión (basada en $\mathbf{G}$). La (clase) función $\mathbf{F}$ definida por $\mathbf{P}$ satisface $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \mid_\alpha)$ para todo α. Es fácil verificar que $\mathbf{F}$ tiene las propiedades requeridas usando la definición de $\mathbf{G}$. ■

La definición de suma de números ordinales es una aplicación del teorema anterior. Para cualquier número ordinal β se define una función $\beta+$.

Definición 9.25 (Suma de Ordinales) Para todo ordinal β,
(a) $\beta + 0 = \beta$.
(b) $\beta + (\alpha + 1) = (\beta + \alpha) + 1$ para todo α,
(c) $\beta + \alpha = \sup\{\beta + \gamma : \gamma < \alpha\}$ para todo ordinal límite $\alpha \neq 0$.

Si hacemos $\alpha = 0$ en *(b)*, tenemos la igualdad $\beta+1 = \beta+1$; el lado izquierdo denota la suma de los números ordinales β y 1, mientras el lado derecho es el sucesor de β.

Para ver cómo la definición de suma es conforme a la versión formal del Teorema de Recursión, consideremos (clase) funciones $\mathbf{G}_1$, $\mathbf{G}_2$ y $\mathbf{G}_3$ donde

$$\mathbf{G}_1(z, x) = z, \quad \mathbf{G}_2(z, x) = x + 1, \quad \mathbf{G}_3(z, x) = \sup(ran\, x).$$

Entonces la forma paramétrica del teorema anterior proporciona una (clase) función $\mathbf{F}$ tal que para todo z

$$\left.\begin{array}{l} \mathbf{F}(z, 0) = \mathbf{G}_1(z, 0) = z. \\ \mathbf{F}(z, \alpha + 1) = \mathbf{G}_2(z, \mathbf{F}_z(\alpha)) = \mathbf{F}(z, \alpha) + 1, \text{ para todo } \alpha. \\ \mathbf{F}(z, \alpha) = \mathbf{G}_3(z, \mathbf{F}_z \restriction \alpha) = \sup(ran\,(\mathbf{F}_z \restriction \alpha)) \\ \qquad\qquad\qquad\qquad = \sup(\{\mathbf{F}(z, \gamma) : \gamma < \alpha\}) \\ \qquad\qquad\qquad\qquad\qquad \text{para } \alpha \neq 0 \text{ límite.} \end{array}\right\} \tag{9.5.2}$$

Si β y α son ordinales, entonces escribimos $\beta + \alpha$ en lugar de $\mathbf{F}(\beta, \alpha)$ y vemos que las condiciones (9.5.2) son exactamente las propiedades (a), (b) y (c) de la definición.

En las subsecuentes aplicaciones del Teorema de Recursión Transfinita usaremos la forma abreviada como en la Definición 9.25, sin explícita formulación de las funciones $\mathbf{G}_1$, $\mathbf{G}_2$ y $\mathbf{G}_3$.

Por otra parte, obsérvese que la definición de suma de números ordinales generaliza la definición de suma para números naturales; de hecho, para números naturales, la parte (c) de la Definición 9.25 no se aplica puesto que ningún número natural distinto de cero es un ordinal límite.

Una consecuencia de 9.25 es que para todo β,

$$(\beta + 1) + 1 = \beta + 2,$$

$$(\beta + 2) + 1 = \beta + 3,$$

etc. También tenemos (si $\alpha = \beta = \omega$)

$$\omega + \omega = \sup\{\omega + n : n < \omega\},$$

y similarmente,

$$(\omega + \omega) + \omega = \sup\{(\omega + \omega) + n : n < \omega\}.$$

En contraste a estos ejemplos, consideremos la suma $m + \omega$ para $m < \omega$. Tenemos $m + \omega = \sup\{m + n : n < \omega\} = \omega$ puesto que si m es un número natural, $m + n$ es también un número natural.

La aritmética de números ordinales es más difícil que la aritmética de números naturales. Una razón de ello es que la conmutatividad no se cumple. Por ejemplo,

$$m + \omega \neq \omega + m.$$

También uno puede ver que, mientras $1 \neq 2$, tenemos que

$$1 + \omega = 2 + \omega.$$

Así, cancelaciones del lado derecho de sumas de ordinales en ecuaciones y desigualdades no son permitidas. Sin embargo, la suma de ordinales es asociativa y se cumple la ley de cancelación izquierda; esto lo probaremos después de establecer algunos resultados previos.

Teorema 9.26 *Si α y β son números ordinales, entonces*

$$\alpha + \beta = \alpha \cup \{\alpha + \gamma : \gamma < \beta\}.$$

Demostración:

La prueba es por inducción sobre β. Supongamos que el teorema es cierto para todo $\gamma < \beta$.

Si $\beta = 0$, por definición $\alpha + \beta = \alpha$. También, si $\beta = 0$,

$$\{\alpha + \gamma : \gamma < \beta\} = \{\alpha + \gamma : \gamma \in \beta\} = \emptyset.$$

Por lo tanto, $\alpha \cup \{\alpha + \gamma : \gamma < \beta\} = \alpha$.

Si β es un ordinal sucesor, digamos $\beta = \gamma + 1$, entonces $\alpha + \beta = (\alpha + \gamma) + 1 = S(\alpha + \gamma)$. Empleando la hipótesis de inducción

$$\begin{aligned} S(\alpha + \gamma) &= S(\alpha \cup \{\alpha + \delta : \delta < \gamma\}) \\ &= (\alpha \cup \{\alpha + \delta : \delta < \gamma\}) \cup \{\alpha \cup \{\alpha + \delta : \delta < \gamma\}\} \\ &= \alpha \cup \{\alpha + \delta : \delta < \gamma\} \cup \{\alpha + \gamma\} \\ &= \alpha \cup \{\alpha + \delta : \delta < \beta\}. \end{aligned}$$

Si β es un ordinal límite. Entonces,

$$\alpha + \beta = \sup\{\alpha + \delta : \delta < \beta\} = \bigcup\{\alpha + \delta : \delta < \beta\} \tag{9.5.3}$$

(recuerde cuál es el supremo de un conjunto de números ordinales). Por lo tanto, $\gamma \in \alpha + \beta$ si y sólo si, existe $\delta \in \beta$ tal que $\gamma \in \alpha + \delta$. Sin embargo, por la hipótesis de inducción, si $\delta \in \beta$, entonces $\gamma \in \alpha + \delta$ si y sólo si $\gamma \in \alpha$ o existe $\delta_1 < \delta$ tal que $\gamma = \alpha + \delta_1$. Por la linealidad de $<$ tenemos que, $\delta_1 < \beta$; consecuentemente,

$$\alpha + \beta \subseteq \alpha \cup \{\alpha + \gamma : \gamma < \beta\}.$$

Por otro lado, de (9.5.3) se deduce que $\alpha \subseteq \alpha + \beta$. Ahora si $\gamma = \alpha + \delta$ para algún $\delta < \beta$, entonces, dado que β es un ordinal límite, $\delta + 1 < \beta$. Por definición

$$\alpha + (\delta + 1) = (\alpha + \delta) + 1 = \gamma + 1,$$

así $\gamma \in \alpha + (\delta + 1)$. Por lo tanto, se sigue de (9.5.3) que $\gamma \in \alpha + \beta$. Luego

$$\alpha \cup \{\alpha + \gamma : \gamma < \beta\} \subseteq \alpha + \beta.$$

Esto completa la demostración. ■

El Teorema 9.26 puede formularse en términos de conjuntos bien ordenados. Dados dos conjuntos ordenados $(A, \leq)$ y $(B, \preceq)$ podemos bien ordenar la unión $A \sqcup B$ (ver Ejercicio 3.2.11) con la relación $\ll$ del Ejercicio 4.5.12.

Teorema 9.27 *Si $(A, \leq)$ y $(B, \preceq)$ son conjunto bien ordenados con tipos de orden $\|(A, \leq)\| = \alpha$ y $\|(B, \preceq)\| = \beta$, entonces $A \sqcup B$ con la relación $\ll$ antes descrita, tiene tipo de orden $\alpha + \beta$.*

Demostración:

Por hipótesis, los conjuntos ordenados $(A, \leq)$ y $(B, \preceq)$ son isomorfos a $(\alpha, \leq)$ y $(\beta, \leq)$, respectivamente. Como

$$\alpha \cap \{\alpha + \gamma : \gamma < \beta\} = \emptyset$$

y el conjunto ordenado $(B, \preceq)$ es isomorfo a $(\{\alpha + \gamma : \gamma < \beta\}, \leq)$, se verifica sin dificultad que $(A \sqcup B, \ll)$ es isomorfo a

$$(\alpha \cup \{\alpha + \gamma : \gamma < \beta\}, \leq).$$

Empleando el Teorema 9.26, $\alpha \cup \{\alpha + \gamma : \gamma < \beta\} = \alpha + \beta$. Por lo tanto, $\|(A \sqcup B, \ll)\| = \alpha + \beta$. ■

Un caso particular del Teorema 9.27 es tomar a $(A, \leq)$ como $(\alpha, \leq)$ y a $(B, \preceq)$ como $(\beta, \leq)$, lo que permite interpretar la suma de ordinales como el tipo de orden del conjunto $(\alpha \sqcup \beta, \ll)$. Se le sugiere al lector interpretar con una gráfica este resultado

Proposición 9.28 *(a) Si α_1, α_2 y β son ordinales, entonces $\alpha_1 < \alpha_2$ si y sólo si $\beta + \alpha_1 < \beta + \alpha_2$.*

(b) Para cualesquiera ordinales α_1, α_2 y β, $\beta + \alpha_1 = \beta + \alpha_2$ si y sólo si $\alpha_1 = \alpha_2$.

(c) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ para todos los ordinales α, β y γ.

DEMOSTRACIÓN:

(a) Por el Teorema 9.26, $\beta + \alpha_1 = \beta \cup \{\beta + \gamma : \gamma < \alpha_1\}$. Por lo tanto, si $\alpha_1 < \alpha_2$, entonces $\beta + \alpha_1 < \beta + \alpha_2$.

Recíprocamente, supongamos que $\beta + \alpha_1 < \beta + \alpha_2$. Si $\alpha_2 < \alpha_1$, la implicación antes probada muestra que $\beta + \alpha_2 < \beta + \alpha_1$. Como $\alpha_1 = \alpha_2$ es también imposible (implica $\beta + \alpha_1 = \beta + \alpha_2$), se concluye por la linealidad de $<$ que $\alpha_1 < \alpha_2$.

(b) Se sigue trivialmente de (a): Si $\alpha_1 \neq \alpha_2$, entonces o bien $\alpha_1 < \alpha_2$ o $\alpha_2 < \alpha_1$ y consecuentemente $\beta + \alpha_1 < \beta + \alpha_2$ o $\beta + \alpha_2 < \beta + \alpha_1$. Si $\alpha_1 = \alpha_2$, entonces obviamente $\beta + \alpha_1 = \beta + \alpha_2$.

(c) Use el Teorema 9.26 y la asociatividad de la unión. Los detalles se dejan como ejercicio al lector. ■

Sabemos que $\alpha_1 < \alpha_2$ no necesariamente implica $\alpha_1 + \beta < \alpha_2 + \beta$, un ejemplo es $1 + \omega = 2 + \omega$; pero podemos establecer un resultado más débil.

Proposición 9.29 *Si α_1, α_2 son números ordinales entonces para cualquier ordinal β, $\alpha_1 < \alpha_2$ implica $\alpha_1 + \beta \leq \alpha_2 + \beta$.*

DEMOSTRACIÓN:

Haremos la demostración por inducción transfinita sobre β. Supóngase que la proposición es cierta para $\delta < \beta$ y supongamos $\alpha_1 < \alpha_2$. Por el Teorema 9.26, $\xi \in \alpha_1 + \beta$ si y sólo si $\xi \in \alpha_1$ o existe $\delta < \beta$ tal que $\xi = \alpha_1 + \delta$. Como $\alpha_1 < \alpha_2$ tenemos que: $\xi < \alpha_1$ implica $\xi < \alpha_2$. Si $\xi = \alpha_1 + \delta$ donde $\delta < \beta$ entonces por la hipótesis de inducción $\xi \leq \alpha_2 + \delta$. En resumen, del Teorema 9.26 se sigue que si $\xi \in \alpha_1 + \beta$ entonces $\xi \in \alpha_2 + \beta$; o sea $\alpha_1 + \beta \subseteq \alpha_2 + \beta$. Luego $\alpha_1 + \beta \leq \alpha_2 + \beta$. ■

Teorema 9.30 *Si α es cualquier número ordinal y β es un ordinal límite, entonces $\alpha + \beta$ es un ordinal límite.*

DEMOSTRACIÓN:

Supóngase que $\gamma \in \alpha + \beta$. Nuevamente usando el Teorema 9.26, o bien $\gamma \in \alpha$ o existe $\delta \in \beta$ tal que $\gamma = \alpha + \delta$. Entonces necesariamente: $\gamma + 1 \in \alpha$ o

$\gamma + 1 = \alpha$ o $\gamma + 1 = (\alpha + \delta) + 1 = \alpha + (\delta + 1)$. Dado que β es un ordinal límite $\delta \in \beta$ implica $\delta + 1 \in \beta$. Por lo tanto, en cualquier caso, $\gamma + 1 \in \alpha + \beta$, es decir, $\alpha+\beta$ es un ordinal límite. ■

Corolario 9.31 *Si α es cualquier número ordinal y β es un ordinal límite, entonces*

$$\alpha + \beta = \sup\{\gamma : \gamma < \alpha + \beta\} = \bigcup\{\gamma : \gamma < \alpha + \beta\}.$$

Finalizamos el estudio de la suma de ordinales con un teorema de utilidad con el cual puede definirse (en algunos casos) la resta de números ordinales.

Teorema 9.32 *Si α y β son números ordinales tales que $\alpha \leq \beta$ entonces existe un único ordinal γ tal que $\alpha + \gamma = \beta$.*

Demostración:

La unicidad se sigue de la ley de cancelación izquierda (Proposición 9.28(b)).

Si $\alpha = \beta$, entonces basta tomar $\gamma = 0$. Supóngase que $\alpha < \beta$, entonces $\beta \setminus \alpha$ es un conjunto no vacío y bien ordenado por $\leq$ restringido a $\beta \setminus \alpha$. Sea $\gamma = \|(\beta \setminus \alpha, \leq)\|$, usando el Teorema 9.27 se sigue que $\alpha + \gamma = \beta$. ■

A continuación damos la definición de multiplicación de ordinales.

Definición 9.33 (Multiplicación de Ordinales) Para todo ordinal β*:*

(a) $\beta \cdot 0 = 0$,

(b) $\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta$ para todo α,

(c) $\beta \cdot \alpha = \sup\{\beta \cdot \gamma : \gamma < \alpha\}$ para todo ordinal límite $\alpha \neq 0$.

Ejemplo 9.34 (a) $\beta \cdot 1 = \beta \cdot (0 + 1) = \beta \cdot 0 + \beta = \beta$.

(b) $\beta \cdot 2 = \beta(1 + 1) = \beta \cdot 1 + \beta = \beta + \beta$, en particular, $\omega \cdot 2 = \omega + \omega$.

(c) $\beta \cdot 3 = \beta \cdot (2 + 1) = \beta \cdot 2 + \beta = \beta + \beta + \beta$.

(d) $\beta \cdot \omega = \sup\{\beta \cdot n : n < \omega\} = \sup\{\beta,\ \beta + \beta,\ \beta + \beta + \beta,\ \ldots\}$

Ejemplo 9.35 $1 \cdot \alpha = \alpha$. Pero esto requiere una demostración inductiva.

Demostración:

Si $\alpha = 0$, entonces $1 \cdot 0 = 0$. También para α sucesor, digamos $\alpha = \gamma + 1$, $1 \cdot (\gamma + 1) = 1 \cdot \gamma + 1 = \gamma + 1 = \alpha$. Finalmente, si $\alpha \neq 0$ es un ordinal límite, $1 \cdot \alpha = \sup\{1 \cdot \gamma : \gamma < \alpha\} = \sup\{\gamma : \gamma < \alpha\} = \alpha$. ■

Ejemplo 9.36 $2 \cdot \omega = \sup\{2 \cdot n : n < \omega\} = \omega$. Como $\omega \cdot 2 \neq \omega$, se concluye que la multiplicación de ordinales generalmente no es conmutativa.

Como en el caso de la suma, es útil describir la multiplicación de números ordinales en términos de conjuntos bien ordenados. Primero un lema cuya demostración se encomienda al lector.

Lema 9.37 *Sean $(X, \leq)$ y $(Y, \preceq)$ conjuntos bien ordenados y sea $\ll_h$ el orden lexicográfico horizontal en $X \times Y$. Entonces:*

(a) W es un segmento inicial de $X \times Y$ si y sólo si existen un segmento inicial U de X y un segmento inicial V de Y tales que

$$W = (X \times V) \cup (U \times \{u\}),$$

donde $u = \min Y \setminus V$.

(b) Si W es un segmento inicial de $X \times Y$, entonces existe un segmento inicial V de Y tal que $X \times V$ es un segmento inicial de $X \times Y$ y $W \subseteq X \times V$.

(c) Si X y Y no tienen elementos máximos, $X \times Y$ tampoco tiene elemento máximo.

Teorema 9.38 *Sean $(X, \leq)$ y $(Y, \preceq)$ conjuntos bien ordenados con tipos de orden α y β, respectivamente. Si $\ll_h$ es el orden lexicográfico horizontal, entonces*

$$\|(X \times Y, \ll_h)\| = \alpha \cdot \beta.$$

Demostración:

Haremos la demostración por inducción transfinita sobre β. Supóngase que el teorema es cierto para todo $\gamma < \beta$.

Si $\beta = 0$, entonces $Y = \emptyset$, por lo tanto, $X \times Y = \emptyset$, así

$$\|(X \times Y, \ll_h)\| = \alpha \cdot \beta.$$

Si $\beta = \gamma + 1$, entonces por el Ejercicio 9.3.4, Y tiene un elemento máximo, digamos u. Sea $Z = Y \setminus \{u\}$. Entonces $\|(Z, \preceq)\| = \gamma$, y por la hipótesis inductiva,

$$\|(X \times Z, \ll_h)\| = \alpha \cdot \gamma.$$

Pero $X \times Y = X \times (Z \cup \{u\}) = (X \times Z) \cup (X \times \{u\})$. Por lo tanto, por el Lema 9.37(a) y la definición de $\ll_h$,

$$\|(X \times Y, \ll_h)\| = \alpha \cdot \gamma + \alpha = \alpha \cdot \beta.$$

Si β es un ordinal límite. Para cada $\gamma < \beta$ existe un único segmento inicial Z de Y tal que

$$\|(Z, \preceq)\| = \gamma.$$

También se sigue del Lema 9.37(a) que $X \times Z$ es un segmento inicial de $X \times Y$. Por lo tanto, la hipótesis inductiva implica

$$\|(X \times Z, \ll_h)\| = \alpha \cdot \gamma.$$

Más aún, puesto que Y no tiene elemento máximo, $X \times Y$ tampoco. Por lo tanto, $\|(X \times Y, \ll_h)\|$ es un ordinal límite, con lo cual

$$\|(X \times Y, \ll_h)\| = \bigcup \{\|(W, \ll_h)\| : W \text{ es segmento inicial de } X \times Y\}.$$

Por el Lema 9.37, para cada W segmento inicial de $X \times Y$, existe un segmento inicial V de Y tal que W está contenido en el segmento inicial $X \times V$ de $X \times Y$; luego

$$\begin{aligned} \|(X \times Y, \ll_h)\| &= \bigcup \{\|(X \times V, \ll_h)\| : V \text{ es segmento inicial de } Y\} \\ &= \bigcup \{\alpha \cdot \gamma : \gamma < \beta\} \\ &= \sup \{\alpha \cdot \gamma : \gamma < \beta\} \\ &= \alpha \cdot \beta. \end{aligned}$$

Lo cual completa la demostración. ■

Si cambiamos el orden lexicográfico horizontal por el orden lexicográfico vertical entonces

$$\|(X \times Y, \ll_v)\| = \beta \cdot \alpha$$

(ver Ejercicios 9.3.3a y 9.5.6).

En los siguientes teoremas estableceremos propiedades de la multiplicación de ordinales. Únicamente se realizarán indicaciones de sus demostraciones y se sugiere que el lector las realice.

Teorema 9.39 *Para cualesquiera ordinales α, β y γ,*

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

DEMOSTRACIÓN:

Use el Teorema 9.38 y el hecho de que $(\alpha \times \beta) \times \gamma$ es equipotente a $\alpha \times (\beta \times \gamma)$. ■

Teorema 9.40 *Si $\alpha \neq 0$ y β es un ordinal límite, o si $\beta \neq 0$ y α es un ordinal límite, entonces $\alpha \cdot \beta$ es un ordinal límite.*

DEMOSTRACIÓN:

Use el Lema 9.37 y el Teorema 9.38. ■

El recíproco del teorema anterior también es cierto. Ver el Ejercicio 9(c) de esta sección.

Teorema 9.41 *Si β es un ordinal límite y $\alpha \neq 0$, entonces*

$$\alpha\beta = \sup\{\gamma : \gamma < \alpha \cdot \beta\}.$$

DEMOSTRACIÓN:

Use el Teorema 9.40, el hecho de que para un ordinal límite α se tiene que $\alpha = \bigcup \alpha$ y la definición. ■

Teorema 9.42 *Si $\alpha \neq 0$ y $\beta < \gamma$, entonces $\alpha \cdot \beta < \alpha \cdot \gamma$.*

DEMOSTRACIÓN:

Se sigue del Lema 9.37(a), del Teorema 9.38 y del hecho de que si $\alpha \neq 0$ y β es un segmento inicial de γ, entonces $\alpha \cdot \beta$ es un segmento inicial de $\alpha \cdot \gamma$. ■

Teorema 9.43 *Si $\alpha \neq 0$ y $\alpha \cdot \beta = \alpha \cdot \gamma$, entonces $\beta = \gamma$.*

DEMOSTRACIÓN:

Use el Teorema 9.42 y la linealidad del (clase) orden $\leq$ en **Ord**. ■

El teorema precedente nos proporciona la ley de cancelación izquierda. La ley de cancelación derecha no se cumple, ya que

$$1 \cdot \omega = \omega = 2 \cdot \omega,$$

pero $1 \neq 2$. Más aún, este mismo ejemplo demuestra que la multiplicación por la izquierda no es monótona: $1 < 2$, pero $1 \cdot \omega = 2 \cdot \omega$. Sin embargo, podemos demostrar el siguiente teorema.

Teorema 9.44 *Si α, β y γ son cualesquiera ordinales, entonces $\alpha < \beta$ implica $\alpha \cdot \gamma \leq \beta \cdot \gamma$.*

Demostración:

"Para variar", la demostración es por inducción transfinita sobre γ. Supóngase que la implicación es cierta para todo $\delta < \gamma$ y supóngase que $\alpha < \beta$.

Si $\gamma = 0$, la implicación es trivial.

Si $\gamma = \delta + 1$, entonces por la hipótesis de inducción, $\alpha \cdot \delta \leq \alpha \cdot \delta$. Más aún, por definición:

$$\begin{aligned} \alpha \cdot \gamma &= \alpha \cdot \delta + \alpha \\ &\leq \beta \cdot \delta + \alpha \\ &\leq \beta \cdot \delta + \beta \\ &= \beta \cdot \gamma. \end{aligned}$$

Si γ es un ordinal límite y $\alpha = 0$, entonces $\alpha \cdot \gamma = 0 \leq \beta \cdot \gamma$. Supongamos entonces que $\alpha \neq 0$. Entonces por el Teorema 9.41 y dado que $\alpha < \beta$, $\alpha \cdot \gamma$ y $\beta \cdot \gamma$ son ordinales límites. Por lo tanto, por definición,

$$\begin{aligned} \alpha \cdot \gamma &= \sup\{\alpha \cdot \delta : \delta < \gamma\} \\ &\leq \sup\{\beta \cdot \delta : \delta < \gamma\} \\ &= \beta \cdot \gamma. \quad \blacksquare \end{aligned}$$

A continuación mostraremos que la multiplicación es distributiva con respecto a la suma por el lado izquierdo. Sin embargo, no es distributiva por el lado derecho, como lo ilustra el siguiente ejemplo:

$$(1+1) \cdot \omega = 2 \cdot \omega = \omega$$

$$(1 \cdot \omega) + (1 \cdot \omega) = \omega + \omega \neq \omega.$$

Teorema 9.45 *Para cualesquiera ordinales α, β y γ se cumple:*

$$\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Demostración:

Sean $(X, \leq_1)$, $(Y, \leq_2)$ y $(Z, \leq_3)$ conjuntos bien ordenados de tipos de orden α, β y γ, respectivamente. Si $\leq$ es el orden de la unión ajena $Y \sqcup Z$ como se dijo en el Teorema 9.27, y $\ll$ es el orden lexicográfico horizontal en $X \times (Y \sqcup Z)$. Entonces

$$\|(X \times (Y \sqcup Z), \ll)\| = \alpha(\beta + \gamma). \tag{9.5.4}$$

Ahora sean $\ll_1$ y $\ll_2$ los órdenes lexicográficos horizontales en $X \times Y$ y $X \times Z$, respectivamente, y $\leq'$ es el orden de la unión ajena $(X \times Y) \sqcup (Y \times Z)$, entonces

$$\left\|\left((X \times Y) \sqcup (X \times Z), \leq'\right)\right\| = \alpha \cdot \gamma + \beta \cdot \gamma. \tag{9.5.5}$$

Se puede verificar que $(X \times (Y \sqcup Z), \ll)$ es isomorfo a

$$\big((X \times Y) \sqcup (X \times Z), \leq'\big)\,.$$

El resultado se sigue de (9.5.4) y (9.5.5). ■

Terminamos la sección definiendo la exponenciación de ordinales y enunciando algunas de sus propiedades.

Definición 9.46 (Exponenciación de Ordinales) Para todo ordinal β,
(a) $\beta^0 = 1$,
(b) $\beta^{\alpha+1} = \beta^\alpha \cdot \beta$ para todo ordinal α,
(c) $\beta^\alpha = \sup\{\beta^\gamma : \gamma < \alpha\}$ para todo ordinal límite $\alpha \neq 0$.

Ejemplo 9.47 (a) $\beta^1 = \beta$, $\beta^2 = \beta \cdot \beta$, $\beta^3 = \beta^2 \cdot \beta = \beta \cdot \beta \cdot \beta$, etc.
(b) $\beta^\omega = \sup\{\beta^n : n < \omega\}$; en particular,
$1^\omega = 1$,
$2^\omega = \omega$, $3^\omega = \omega$, $\ldots, n^\omega = \omega$ para cualquier $n \in \omega$.
$\omega^\omega = \sup\{\omega^n : n < \omega\} > \omega$.

Teorema 9.48 *Si $\beta > 1$ y α es un ordinal límite, entonces β^α es un ordinal límite.*

Teorema 9.49 *Para cualesquiera ordinales α, β y γ,*

$$\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma \quad \text{y} \quad (\alpha^\beta)^\gamma = \alpha^{\beta\gamma}.$$

Puesto que la multiplicación de números ordinales no es conmutativa, no es cierto que $(\alpha\beta)^\gamma = \alpha^\gamma \cdot \alpha^\beta$ para cualesquiera ordinales α, β y γ. Para ver esto, sea $\alpha = \omega$ y $\beta = \gamma = 2$. Entonces

$$\begin{aligned}(\omega \cdot 2)^2 &= (\omega \cdot 2) \cdot (\omega \cdot 2)\\ &= \omega \cdot (2 \cdot \omega) \cdot 2\\ &= (\omega \cdot \omega) \cdot 2\\ &= \omega^2 \cdot 2.\end{aligned}$$

Sin embargo, $\omega^2 \cdot 2^2 = \omega^2 \cdot 4 \neq \omega^2 \cdot 2$.

Se puede destacar que la aritmética ordinal difiere sustancialmente de la aritmética de números cardinales. Por ejemplo, $2^\omega = \omega$ y ω^ω son ordinales numerables, mientras $2^{\aleph_0} = \aleph_0^{\aleph_0}$ es no numerable.

Uno puede usar las operaciones aritméticas para generar ordinales cada vez más grandes:

$$0,\ 1,\ 2,\ 3,\ \ldots\ ,\ \omega,\ \omega+1,\ \omega+2,\ \ldots,\ \omega\cdot 2,\ \omega\cdot 2+1,\ \ldots,$$
$$\omega\cdot 3,\ \ldots,\ \omega\cdot 4,\ \ldots,\ \omega\cdot\omega=\omega^2,\ \omega^2+1,\ \ldots,\ \omega^2+\omega,\ \ldots,$$
$$\omega^2\cdot 2,\ \ldots,\ \omega^3,\ \ldots\omega^4,\ \ldots,\ \omega^\omega,\ \omega^\omega+1,\ \ldots,\ \omega^\omega\cdot 2,\ \ldots,$$
$$\omega^\omega\cdot\omega=\omega^{\omega+1},\ \ldots,\ \omega^{\omega^2},\ \ldots,\ \omega^{\omega^3},\ \ldots,\ \omega^{\omega^\omega},\ \ldots,\ \omega^{\omega^{\omega^\omega}},\ \ldots$$

El proceso puede fácilmente ser continuado. Es costumbre definir

$$\epsilon=\sup\left\{\omega,\ \omega^\omega,\ \omega^{\omega^\omega},\ \ldots\right\}.$$

Uno puede entonces formar $\epsilon+1,\ \epsilon+\omega,\ \epsilon^\omega,\ \epsilon^\epsilon,\ \epsilon^{\epsilon^\epsilon}$, etc.

Ejercicios 9.5

1. Evalúe las siguientes operaciones:

   (a) $(\omega+1)+\omega$.

   (b) $\omega+\omega^2$.

   (c) $(\omega+1)\cdot\omega^2$.

2. Pruebe que para cada ordinal α existen un único ordinal límite β y un único número natural n tal que $\alpha=\beta+n$. (Sugerencia:

   $$\beta=\sup\left\{\gamma\leq\alpha:\gamma\text{ es límite}\right\}.)$$

3. Sean $\alpha\leq\beta$ ordinales. Muestre que la ecuación $\xi+\alpha=\beta$ puede tener 0, 1 o infinitas soluciones.

4. Complete la demostración de la Proposición 9.28(c).

5. Demuestre el Lema 9.37.

6. Demuestre que si $(X,\leq)$ y $(Y,\leq)$ son conjuntos bien ordenados con tipos de orden α y β, respectivamente, entonces el tipo de orden de

   $$(X\times Y,\ll_v)$$

   es $\beta\cdot\alpha$.

7. Pruebe cada uno de las siguientes implicaciones.

   (a) $\alpha \neq 0$ y $\beta \neq 0$ implica $\alpha \cdot \omega^\beta = (\alpha + 1) \cdot \omega^\beta$.
   (b) $\alpha\beta < \alpha\gamma$ implica $\beta < \gamma$.
   (c) $\alpha \cdot \beta = 0$ si y sólo si $\alpha = 0$ o $\beta = 0$.

8. Demuestre los Teoremas 9.39 a 9.43.

9. Demuestre cada una de las siguientes proposiciones.

   (a) α es un ordinal límite si y sólo si $\alpha = \omega \cdot \beta$ para algún β.
   (b) Si α no es un ordinal límite, entonces existe un único ordinal β y un único número natural $n \neq 0$ tal que $\alpha = \omega \cdot \beta + n$.
   (c) Si $\alpha\beta \neq 0$ es un ordinal límite, entonces $\alpha \neq 0$ y β es un ordinal límite, o $\beta \neq 0$ y α es un ordinal límite.

10. Demuestre cada una de las siguientes proposiciones.

    (a) Si $1 < \alpha$ y $\beta < \gamma$, entonces $\alpha^\beta < \alpha^\gamma$.
    (b) Si $\alpha < \beta$, entonces $\alpha^\beta \leq \alpha^\gamma$.
    (c) Si $\alpha^\beta \leq \alpha^\gamma$, entonces $\beta < \gamma$.
    (d) Si $\alpha^\gamma < \beta^\gamma$, entonces $\alpha < \beta$.
    (e) Si $\alpha > 1$ y $\beta > 0$, entonces $\alpha\beta \leq \alpha^\beta$.
    (f) Si $\alpha > 0$ y $\beta > 1$, entonces $\alpha \leq \beta^\alpha$.
    (g) Si $\alpha < \omega^\delta$ y $\beta < \omega^\delta$, entonces $\alpha + \beta < \omega^\delta$.
    (h) Si $\alpha < \omega^{\omega^\delta}$ y $\beta < \omega^{\omega^\delta}$, entonces $\alpha \cdot \beta < \omega^{\omega^\delta}$.
    (i) Si $n \in \omega$, $n \neq 0$ y $\alpha \neq 0$, entonces $n\omega^\alpha = \omega^\alpha$.

11. Supóngase que $\alpha = \sup\{\gamma_\xi : \xi < \zeta\}$. Demuestre que

    (a) $\beta + \alpha = \sup\{\beta + \gamma_\xi : \xi < \zeta\}$,
    (b) $\beta \cdot \alpha = \sup\{\beta \cdot \gamma_\xi : \xi < \zeta\}$,
    (c) $\beta^\alpha = \sup\{\beta^{\gamma_\xi} : \xi < \zeta\}$.

12. Encuentre un conjunto de A de números racionales tales que $(A, \leq_Q)$ sea isomorfo a $(\alpha, \leq)$, donde

    (a) $\alpha = \omega + 1$,

(b) $\alpha = \omega \cdot 2$,

(c) $\alpha = \omega \cdot 3$,

(d) $\alpha = \omega^{\omega}$,

(e) $\alpha = \epsilon$.

(Sugerencia: $\left\{n - \frac{1}{m} : m \in \mathbf{N} \setminus \{0\}\right\}$ es isomorfo a ω^2, etc.)

13. Demuestre que si $(\alpha, \leq)$ es isomorfo a algún conjunto de números reales X (ordenado por la restricción del orden usual en $\mathbf{R}$) entonces α es a lo más numerable. (Sugerencia: sea f un isomorfismo; para cada $\gamma < \alpha$, use el intervalo

$$I_\gamma = \{x \in \mathbf{R} : f(\gamma) < x < f(\gamma + 1)\}$$

y la densidad de los racionales.)

14. (Caracterización de la Exponenciación.) Sean α y β números ordinales. Para cada $f : \beta \to \alpha$, sea $s(f) = \{\gamma < \beta : f(\gamma) = 0\}$. Sea $s(\beta, \alpha) = \{f : \beta \to \alpha : s(f) \text{ es finito}\}$. Defínase una relación de orden $\prec$ en $s(\beta, \alpha)$ como sigue: $f \prec g$ si y sólo si existe $\gamma_0 < \beta$ tal que $f(\gamma_0) < g(\gamma_0)$ y $f(\gamma) = g(\gamma)$ para todo $\gamma \leq \gamma_0$. Muestre que $(s(\beta, \alpha), \prec)$ es isomorfo a $(\alpha^\beta, <)$.

15. Demuestre los Teoremas 9.48 y 9.49.

9.6 Ordinales Iniciales y Alephs

En el Capítulo 7 empezamos la investigación del concepto de cardinalidad. Hasta ahora hemos demostrado varios resultados que tienen que ver con el concepto $|X|$, la cardinalidad del conjunto X, pero no hemos definido explícitamente el objeto $|X|$, excepto para el caso cuando X es finito o numerable.

En la presente sección consideraremos el problema de encontrar "representantes" de cardinalidad. Puesto que los números naturales desempeñan bien este papel, generalizaremos el método apoyados en los números ordinales. Sin embargo, los números ordinales no representan cardinalidades, más bien, ellos representan a los conjuntos bien ordenados. Como cualquier conjunto infinito puede bien ordenarse de muchas maneras distintas, hay muchos números ordinales de la misma cardinalidad; ω, $\omega + 1$, $\omega + \omega$, $\omega \cdot \omega$, $\omega \cdot \omega + 1$, etc. son todos numerables; esto es, $|\omega| = |\omega + 1| = |\omega + \omega| = |\omega \cdot \omega| = \aleph_0$.

A pesar de estas dificultades, es fácil obtener representantes para la cardinalidad de conjuntos infinitos; simplemente tomaremos el *mínimo* número ordinal de una cardinalidad dada como el representante de esa cardinalidad.

Definición 9.50 Un número ordinal α se llama *ordinal inicial* si no es equipotente a cualquier $\beta < \alpha$.

En otras palabras, α es un ordinal inicial si α equipotente a β implica $\beta \geq \alpha$.

Ejemplo 9.51 Cada número natural es un ordinal inicial. ω es un ordinal inicial, puesto que ω no es equipotente a cualquier número natural. $\omega + 1$ no es un ordinal inicial. Similarmente, tampoco lo son $\omega + \omega$, $\omega \cdot \omega$, ω^ω.

Teorema 9.52 *Todo conjunto bien ordenado es equipotente a un único ordinal inicial.*

Demostración:

Ya sabemos que si $(X, \leq)$ es un conjunto bien ordenado, entonces X es equipotente a algún número ordinal. Sea α_0 el primer ordinal equipotente a X. Entonces α_0 es un ordinal inicial, porque si α_0 es equipotente a β para algún $\beta < \alpha$ entonces X es equipotente a β, contradiciendo la elección de α_0.

Si $\alpha_0 \neq \alpha_1$ son ordinales iniciales, éstos no pueden ser equipotentes, puesto que si lo son, y digamos, $\alpha_0 < \alpha_1$, entonces α_1 no cumple con la definición de ordinal inicial. ■

Usando el Axioma de Elección podemos derivar el siguiente corolario que nos permite definir de manera precisa a $|X|$ para cualquier conjunto X y justificar rigurosamente la Suposición 7.23.

Corolario 9.53 *El Axioma de Elección implica que todo conjunto es equipotente a un ordinal inicial.*

Definición 9.54 Si X es un conjunto, el *número cardinal de X,* denotado por $|X|$, es el único ordinal inicial equipotente a X. En particular, $|X| = \omega$ para cualquier conjunto numerable y $|X| = n$ para cualquier conjunto finito de n elementos; en consistencia con las definiciones previas.

Puesto que $\in$ es un orden lineal (de hecho, un buen orden) en cualquier conjunto de números ordinales, también tenemos el siguiente corolario.

Corolario 9.55 *El Axioma de Elección implica que para cualesquiera conjuntos A y B o bien $|A| \leq |B|$ o $|B| \leq |A|$, es decir, el (clase) orden $\leq$ es lineal.*

De acuerdo al último teorema los números cardinales son precisamente los ordinales iniciales. Una cuestión natural es: ¿Hay ordinales iniciales diferentes de los números naturales y ω? El siguiente teorema muestra mucho más; sin hacer uso del Axioma de Elección, nos dice que hay ordinales iniciales arbitrariamente grandes.

Definición 9.56 Para cualquier conjunto A, sea $\hbar(A)$ el mínimo número ordinal que no es equipotente a cualquier subconjunto de A. Llamaremos a $\hbar(A)$ *número de Hartog de A.*

Por definición, $\hbar(A)$ es el mínimo ordinal α tal que $|\alpha| \not\leq |A|$. Por otra parte, del Axioma de Elección se sigue que el número de Hartog existe para cualquier conjunto A; pero también es posible establecer una demostración sin emplear dicho axioma (ver Ejercicio 9.6.4).

Lema 9.57 *Para todo conjunto A, $\hbar(A)$ es un ordinal inicial.*

Demostración:

Supongamos que β es equipotente a $\hbar(A)$ para algún $\beta < \hbar(A)$. Entonces β es equipotente a un subconjunto de A, por lo que se concluye que $\hbar(A)$ es equipotente a un subconjunto de A, contradiciendo su definición. ■

Ahora estamos interesados en definir, por recursión transfinita, una "escala" de ordinales iniciales.

Definición 9.58

$$\omega_0 = \omega;$$

$$\omega_{\alpha+1} = \hbar(\omega_\alpha) \quad \text{para todo } \alpha;$$

$$\omega_\alpha = \sup\{\omega_\beta : \beta < \alpha\} \quad \text{si } \alpha \neq 0\text{es un ordinal límite.}$$

Note que de la Definición 9.56 se sigue que, para cada ordinal α, $|\omega_{\alpha+1}| > |\omega_\alpha|$ y que $|\omega_\alpha| < |\omega_\beta|$ siempre que $\alpha < \beta$.

Teorema 9.59 *(a) ω_α es un número ordinal inicial infinito para cada α.*

(b) Si Ω es un número ordinal inicial infinito, entonces $\Omega = \omega_\alpha$ para algún α.

DEMOSTRACIÓN:

(a) Se hará por inducción sobre α. El único caso no trivial es cuando $\alpha \neq 0$ es un ordinal límite (por definición y por el lema). Supóngase que $|\omega_\alpha| = |\gamma|$ para algún $\gamma < \omega_\alpha$, entonces existe un $\beta < \alpha$ tal que $\gamma < \omega_\beta$ (por definición de supremo). Pero, puesto que α es un ordinal límite si $\beta < \alpha$ también $\beta + 1 < \alpha$, y esto implica que

$$|\omega_\alpha| = |\gamma| = |\omega_\beta| < |\omega_{\beta+1}| \leq |\omega_\alpha|\,,$$

que es una contradicción.

(b) Por inducción se verifica que $\alpha \leq \omega_\alpha$ para cada α. Suponiendo este preliminar, para todo ordinal inicial infinito Ω existe α tal que $\Omega \leq \omega_\alpha$ (por ejemplo $\alpha = \Omega + 1$). Así, es suficiente mostrar que para cada ordinal inicial $\Omega \leq \omega_\alpha$, hay un ordinal $\gamma \leq \alpha$ tal que $\Omega = \omega_\gamma$.

La demostración procede por inducción sobre α. Supóngase que la propiedad es cierta para todo $\beta < \alpha$.

Si $\alpha = 0$, la afirmación es trivialmente cierta.

Si $\alpha = \beta + 1$ y $\Omega < \omega_\alpha = \hbar(\omega_\beta)$, entonces $\Omega \leq \omega_\beta$. Por la hipótesis de inducción, existe $\gamma \leq \beta < \alpha$ tal que $\Omega = \omega_\gamma$.

Si $\alpha \neq 0$ es un ordinal límite y $\Omega < \omega_\alpha = \sup\{\omega_\beta : \beta < \alpha\}$, entonces por definición de supremo, existe $\beta < \alpha$ tal que $\Omega < \omega_\beta \leq \omega_\alpha$ y nuevamente la hipótesis inductiva nos proporciona un $\gamma < \alpha$ tal que $\Omega = \omega_\gamma$. ■

Usando el Axioma de Elección, la conclusión de esta sección es que cualquier conjunto infinito es equipotente a un único número ordinal inicial y que los números ordinales iniciales son precisamente de la forma

$$\omega_\alpha$$

cuando α varía en toda la clase **Ord**. Los ordinales iniciales son, por definición, la cardinalidad de los conjuntos infinitos. Es costumbre llamar a estos números ordinales *alephs*, y definir

$$\aleph_\alpha = \omega_\alpha$$

para cada $\alpha \in \mathbf{Ord}$.

Los números cardinales son o bien números naturales o alephs. En particular $|\mathbf{N}| = \aleph_0$ coincidiendo con nuestro acuerdo previo. El lector también puede notar que el orden de los números cardinales por "tamaño", como se hizo en el Capítulo 7, coincide con el orden de los números naturales y con el orden de los alephs como ordinales, es decir, si $|X| = \aleph_\alpha$ y $|Y| = \aleph_\beta$, entonces $|X| < |Y|$

si y sólo si $\aleph_\alpha < \aleph_\beta$ (o sea $\omega_\alpha \in \omega_\beta$), y similar equivalencia se cumple si uno o ambos son números naturales.

En el Capítulo 7 definimos la suma, multiplicación y exponenciación de números cardinales; estas operaciones desafortunadamente son poco compatibles con las correspondientes suma, multiplicación y exponenciación como números ordinales. Por ejemplo, $\omega_\alpha + \omega_\alpha \neq \omega_\alpha$ si $+$ es la suma de ordinales, pero $\omega_\alpha + \omega_\alpha = \omega_\alpha$ si $+$ es la suma de cardinales. La suma de cardinales es conmutativa, pero la de ordinales no. Para evitar confusiones, *se usan los símbolos ω_α cuando se trata de operaciones ordinales y los símbolos $\aleph_\alpha$ cuando se refiere a los operaciones cardinales.*

Por otra parte, el lector podrá demostrar sin dificultad que el conjunto de todos los números cardinales no existe. Denotaremos por **Car** a la clase de todos los números cardinales.

Uno puede comparar conjuntos por su cardinalidad, es decir, definir las relaciones $|X| < |Y|$ y $|X| = |Y|$, sin definir el símbolo $|X|$. Con el Axioma de Elección, cualquier conjunto es equipotente a un único aleph, y así uno puede definir $|X|$ como el aleph correspondiente. Sin el Axioma de Elección es imposible hacer una definición del símbolo $|X|$ en **ZF**. Una de las razones de porque usar los alephs para definir la cardinalidad de conjuntos, si se acepta el Axioma de Elección, es que para cualquier ordinal α, $\aleph_\alpha = |\omega_\alpha|$, y así la cardinalidad de $\aleph_\alpha$ es $\aleph_\alpha$. En otras palabras, los números cardinales son representantes de las "clases de equivalencia" de conjuntos de la misma cardinalidad.

Finalmente comentaremos que existe también una definición alternativa de $|X|$ usando el Axioma de Fundación y el concepto de rango de un conjunto que no trataremos aquí pero puede que encontrarse en [R_2].

Ejercicios 9.6

1. Pruebe que para cada α, $\alpha \leq \omega_\alpha$.

2. Sea X un conjunto numerable de ordinales estrictamente menores que ω_1. Use el Axioma de Elecciones Numerables para mostrar que $\sup X < \omega_1$.

3. Pruebe que si α y β son ordinales a lo más numerables, entonces $\alpha + \beta$, $\alpha \cdot \beta$ y α^β son a lo más numerables. (Sugerencia: Use las caracterizaciones de las operaciones en términos de conjuntos bien ordenados o bien use inducción transfinita.)

4. Pruebe sin usar el Axioma de Elección que $\hbar(A)$ existe para cada A. (Sugerencia: hay un único ordinal α isomorfo a Y, donde Y es un subconjunto bien ordenado de A. Use el Axioma Esquema de Reemplazo para tener un conjunto de ordinales isomorfos a cualquier subconjunto bien ordenado de A.)

5. Muestre que para cualquier conjunto A, $|A| < |A| + \hbar(A)$.

6. Sea $\hbar^*(A)$ el mínimo ordinal α tal que no existen funciones sobreyectivas de A en α. Demuestre que:

   (a) Si $\alpha \geq \hbar^*(A)$, entonces no existen sobreyecciones de A en α.
   (b) $\hbar(A) \leq \hbar^*(A)$.
   (c) Si A es bien ordenable, entonces $\hbar(A) = \hbar^*(A)$.
   (d) $\hbar^*(A)$ existe para todo A sin usar el Axioma de Elección. (Sugerencia: muestre que $\alpha \in \hbar^*(A)$ si y sólo si $\alpha = 0$ o α es igual al ordinal isomorfo a W, donde W es un buen orden de alguna partición de A en clases de equivalencia.)

7. Demuestre que si $\alpha > 0$, entonces $\omega_\alpha = \omega^{\omega_\alpha}$. Los números con esta propiedad de llaman *números épsilon*.

8. Encuentre dos conjuntos bien ordenados tales que:

   (a) Cada segmento inicial es finito.
   (b) Cada segmento inicial es a lo más numerable.

9. Muestre que **Car** no es un conjunto.

9.7 Suma y Multiplicación de Alephs

La aritmética de números infinitos difiere sustancialmente de la aritmética de números finitos y de hecho las reglas para sumar y multiplicar alephs es muy simple. Por ejemplo:

$$\aleph_0 + n = \aleph_0$$

para cualquier número natural n (si aumentamos n elementos a un conjunto numerables el resultado es un conjunto numerable.) También tenemos que

$$\aleph_0 + \aleph_0 = \aleph_0$$

ya que, por ejemplo, podemos ver al conjunto de los números naturales como la unión de dos conjuntos numerables ajenos: los pares y los impares. Más aún,

$$\aleph_0 \cdot \aleph_0 = \aleph_0.$$

El conjunto de todas las parejas de números naturales es numerable. Ahora probaremos un teorema general que determina completamente el resultado de la suma y la multiplicación de alephs.

Teorema 9.60 $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$, *para todo* α.

Demostración:

El teorema se probará por inducción transfinita. Para todo α, construiremos un buen orden conveniente $\preceq$ en el conjunto $\omega_\alpha \times \omega_\alpha$, y usaremos la hipótesis de inducción, $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$ para todo $\beta < \alpha$, para concluir que el tipo de orden del conjunto bien ordenado $(\omega_\alpha \times \omega_\alpha, \preceq)$ es a lo más ω_α; con esto, se seguirá que $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$. Puesto que $\aleph_\alpha \cdot \aleph_\alpha \geq \aleph_\alpha$, podemos concluir que $\aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha$.

La primera tarea es construir un buen orden para $\omega_\alpha \times \omega_\alpha$, para todo α. La manera de realizar esto es definir una relación $\preceq$ que será un buen orden en cualquier conjunto de pares de ordinales, y así entonces, $(\omega_\alpha \times \omega_\alpha, \preceq)$ será un conjunto bien ordenado.

Definamos $(\alpha_1, \alpha_2) \prec (\beta_1, \beta_2)$ si y sólo si:

$$\max\{\alpha_1, \alpha_2\} < \max\{\beta_1, \beta_2\}$$

o

$$\max\{\alpha_1, \alpha_2\} = \max\{\beta_1, \beta_2\} \quad \text{y} \quad \alpha_1 < \beta_1$$

o bien

$$\max\{\alpha_1, \alpha_2\} = \max\{\beta_1, \beta_2\} \quad \text{y} \quad \alpha_1 = \beta_1 \quad \text{y} \quad \alpha_2 < \beta_2.$$

Veamos que $\prec$ es transitivo. Sean $\alpha_1,\ \alpha_2,\ \beta_1,\ \beta_2,\ \gamma_1$ y γ_2 tales que

$$(\alpha_1, \alpha_2) \prec (\beta_1, \beta_2) \prec (\gamma_1, \gamma_2).$$

Se sigue de la definición de $\prec$ que

$$\max\{\alpha_1, \alpha_2\} \leq \max\{\beta_1, \beta_2\} \leq \max\{\gamma_1, \gamma_2\};$$

por lo que, $\max\{\alpha_1, \alpha_2\} \leq \max\{\gamma_1, \gamma_2\}$.

Si $\max\{\alpha_1,\alpha_2\} < \max\{\gamma_1,\gamma_2\}$ entonces $(\alpha_1,\alpha_2) \prec (\gamma_1,\gamma_2)$. Supongamos que $\max\{\alpha_1,\alpha_2\} = \max\{\gamma_1,\gamma_2\}$, entonces $\alpha_1 \leq \beta_1 \leq \gamma_1$. Si $\alpha_1 < \gamma_1$ se obtiene $(\alpha_1,\alpha_2) \prec (\gamma_1,\gamma_2)$. De otro modo tenemos que $\alpha_1 = \beta_1 = \gamma_1$, así que necesariamente $\alpha_2 < \beta_2 < \gamma_2$; se sigue nuevamente que $(\alpha_1,\alpha_2) \prec (\gamma_1,\gamma_2)$.

La asimetría de $\prec$ es clara a partir de su definición. Veamos pues que $\preceq$ es un buen orden.

Sea $X \neq \emptyset$ un conjunto de pares de ordinales y sea

$$\delta = \min\{\max\{\alpha,\beta\} : (\alpha,\beta) \in X\}.$$

Luego sea $Y = \{(\alpha,\beta) \in X : \max\{\alpha,\beta\} = \delta\}$. Note que $Y \neq \emptyset$ (pues existe al menos un $(\alpha,\beta) \in X$ tal que $\max\{\alpha,\beta\} = \delta$). $\delta < \max\{\alpha,\beta\}$ para todo $(\alpha,\beta) \in X \setminus Y$ y por lo tanto,

$$(\alpha,\beta) \prec (\alpha',\beta')$$

siempre que $(\alpha,\beta) \in Y$ y $(\alpha',\beta') \in X \setminus Y$. Por lo tanto, el $\preceq$-mínimo elemento de Y, si existe, es también el mínimo elemento de X. Sean

$$\alpha_0 = \min\{\alpha : (\alpha,\beta) \in Y\} \quad \text{y} \quad Z = \{(\alpha,\beta) \in Y : \alpha = \alpha_0\}.$$

El conjunto Z es no vacío y $(\alpha,\beta) \preceq (\alpha',\beta')$ siempre que $(\alpha,\beta) \in Z$ y $(\alpha',\beta') \in Y$. Finalmente tomemos $\beta_0 = \min\{\beta : (\alpha,\beta) \in Z\}$. Claramente, $(\alpha_0,\beta_0) = \min Z$ y se sigue que $(\alpha_0,\beta_0) = \min X$.

Teniendo demostrado que $\preceq$ es un buen orden para cualquier conjunto de pares de ordinales, se sigue que es un buen orden para $\omega_\alpha \times \omega_\alpha$ (para todo α). Usaremos esto para probar por inducción transfinita sobre α que $|\omega_\alpha \times \omega_\alpha| \leq \aleph_\alpha$.

Ya sabemos que $\aleph_0 \cdot \aleph_0 = \aleph_0$, así la afirmación es cierta para $\alpha = 0$. Sea $\alpha > 0$ y supongamos que $\aleph_\beta \cdot \aleph_\beta \leq \aleph_\beta$ para todo $\beta < \alpha$.

Para demostrar que $|\omega_\alpha \times \omega_\alpha| \leq \aleph_\alpha$ es suficiente mostrar que el tipo de orden del conjunto bien ordenado $(\omega_\alpha \times \omega_\alpha, \preceq)$ es a lo más ω_α.

Si el tipo de orden de $\omega_\alpha \times \omega_\alpha$ fuera mayor que ω_α, entonces debería existir $(\alpha_1,\alpha_2) \in \omega_\alpha \times \omega_\alpha$ tal que la cardinalidad del segmento inicial determinado por (α_1,α_2),

$$X_{(\alpha_1,\alpha_2)} = \{(\gamma_1,\gamma_2) \in \omega_\alpha \times \omega_\alpha : (\gamma_1,\gamma_2) \prec (\alpha_1,\alpha_2)\},$$

es $\aleph_\alpha$. Consecuentemente, es suficiente probar que para todo $(\alpha_1,\alpha_2) \in \omega_\alpha \times \omega_\alpha$ se tiene que $\left|X_{(\alpha_1,\alpha_2)}\right| < \aleph_\alpha$.

Sean $(\alpha_1,\alpha_2) \in \omega_\alpha \times \omega_\alpha$ y $\beta = \max\{\alpha_1,\alpha_2\} + 1$. Entonces $\beta \in \omega_\alpha$ y para todo $(\gamma_1,\gamma_2) \in X(\alpha_1,\alpha_2)$,

$$\max\{\gamma_1,\gamma_2\} \leq \max\{\alpha_1,\alpha_2\} < \beta.$$

A partir de esta última relación se deduce que γ_1, $\gamma_2 \in \beta$. Por tanto, $X_{(\alpha_1,\alpha_2)} \subseteq \beta \times \beta$.

Sea $\gamma < \alpha$ tal que $|\beta| \leq \aleph_\gamma$ (note que es posible elegir γ ya que ω_α es un ordinal inicial), entonces $\left|X_{(\alpha_1,\alpha_2)}\right| \leq |\beta \times \beta| = |\beta| \cdot |\beta| \leq \aleph_\gamma \cdot \aleph_\gamma$. Pero, por la hipótesis inductiva, $\aleph_\gamma \cdot \aleph_\gamma \leq \aleph_\gamma$; por lo tanto, $\left|X_{(\alpha_1,\alpha_2)}\right| \leq \aleph_\gamma < \aleph_\alpha$.

Ahora se sigue que $|\omega_\alpha \times \omega_\alpha| \leq \aleph_\alpha$. Así tenemos probado por inducción transfinita que $\aleph_\alpha \cdot \aleph_\alpha \leq \aleph_\alpha$ para todo α. ■

Terminemos esta sección enumerando algunas consecuencias del Teorema 9.60.

Corolario 9.61 *Para cualquier α y β tales que $\alpha \leq \beta$,*

$$\aleph_\alpha \cdot \aleph_\beta = \aleph_\beta.$$

También,

$$n \cdot \aleph_\alpha = \aleph_\alpha$$

para todo número natural n.

Demostración:

Si $\alpha \leq \beta$, entonces, por un lado, $\aleph_\beta = 1 \cdot \aleph_\beta \leq \aleph_\alpha \cdot \aleph_\beta$, y por otro lado, por el Teorema 9.60, $\aleph_\alpha \cdot \aleph_\beta \leq \aleph_\beta \cdot \aleph_\beta = \aleph_\beta$. Similarmente, $n \cdot \aleph_\alpha = \aleph_\alpha$. ■

Corolario 9.62 *Para todo α y β tales que $\alpha \leq \beta$,*

$$\aleph_\alpha + \aleph_\beta = \aleph_\beta.$$

También

$$n + \aleph_\alpha = \aleph_\alpha$$

para todo número natural n.

Demostración:

Si $\alpha \leq \beta$, entonces $\aleph_\beta \leq \aleph_\alpha + \aleph_\beta \leq \aleph_\beta + \aleph_\beta = 2 \cdot \aleph_\beta = \aleph_\beta$. La segunda parte se demuestra de manera similar. ■

Ejercicios 9.7

1. Demuestre que:

   (a) $\aleph_\alpha^n = \aleph_\alpha$ para todo número natural n.

   (b) $|[\aleph_\alpha]^n| = \aleph_\alpha$, donde $[\aleph_\alpha]^n$ es la familia de todos los subconjuntos de ω_α formados de n elementos.

   (c) $\left|[\aleph_\alpha]^{<\aleph_0}\right| = \aleph_\alpha$, donde $[\aleph_\alpha]^{<\aleph_0}$ es la familia de todos los subconjuntos finitos de ω_α.
   (Sugerencia: use el Teorema 9.60 e inducción.)

2. Si α y β son ordinales y $|\alpha| \leq \aleph_\gamma$ y $|\beta| \leq \aleph_\gamma$, entonces $|\alpha + \beta| \leq \aleph_\gamma$, $|\alpha \cdot \beta| \leq \aleph_\gamma$, $\left|\alpha^\beta\right| \leq \aleph_\gamma$ (donde $\alpha + \beta$, $\alpha \cdot \beta$ y α^β son las operaciones ordinales).

3. Si X es un subconjunto de ω_α tal que $|X| < \aleph_\alpha$, entonces $|\omega_\alpha \setminus X| = \aleph_\alpha$.

4. Demuestre que

   (a) $\left|[\aleph_\alpha]^{\leq\aleph_\beta}\right| \leq \aleph_\alpha^{\aleph_\beta}$, donde $[\aleph_\alpha]^{\leq\aleph_\beta}$es la familia de todos los subconjuntos de ω_α de cardinalidad menor o igual a $\aleph_\beta$.

   (b) $\left|[\aleph_\alpha]^{\aleph_\beta}\right| = \aleph_\alpha^{\aleph_\beta}$, donde $[\aleph_\alpha]^{\aleph_\beta}$ es la familia de todos los subconjuntos de ω_α de cardinalidad $\aleph_\beta$.

   (c) $\left|\left\{f \in \omega_\alpha^A : A \in [\aleph_\alpha]^{\leq\aleph_\beta}\,,\ f \text{ es inyectiva}\right\}\right| = \aleph_\alpha^{\aleph_\beta}$.

5. Demuestre que la cardinalidad del conjunto de todos los ordinales sucesores menores que ω_α tiene cardinalidad $\aleph_\alpha$.

6. ¿Cuántos buenos órdenes no isomorfos pueden definirse sobre $\mathbf{N}$? (Sugerencia: ver Ejercicio 9.4.6.)

10

Teoría de Cardinales

En el Capítulo 7 se introdujo la noción de cardinalidad y se asumió la existencia de un conjunto $|X|$, llamado el número cardinal de X. En la Sección 9.6 se formalizó, para cada conjunto X, la existencia del conjunto $|X|$ por medio del Axioma de Elección y también se observó que es imposible hacer una definición del símbolo $|X|$ sin emplear a dicho axioma. Por otra parte, en la Sección 9.7 se determinó por completo la aritmética de alephs; pero, sin emplear al Axioma de Elección, *tener determinada la aritmética de alephs no implica tener determinada la aritmética de números cardinales.* En este capítulo mostraremos la estrecha relación entre el Axioma de Elección y los números cardinales, probaremos algunas equivalencias del axioma en términos de cardinales y desarrollaremos temas especiales de la Teoría de Cardinales.

10.1 Números Cardinales y el Axioma de Elección

En Teoría de Conjuntos con el Axioma de Elección, cualquier conjunto es equipotente a un aleph y los alephs (como clase) son bien ordenados. Sin el Axioma de Elección, sin embargo, no es posible demostrar que el ordenamiento $|X| \leq |Y|$, sea un orden lineal en la clase de todos los números cardinales. En la Sección 7.3 se estableció que el ordenamiento $\leq$ tiene las siguientes propiedades para cualesquiera conjuntos X, Y, Z:

(a) $|X| \leq |X|$;

(b) si $|X| \leq |Y|$ y $|Y| \leq |X|$, entonces $|X| = |Y|$;

(c) si $|X| \leq |Y|$ y $|Y| \leq |Z|$, entonces $|X| \leq |Z|$.

Así, $\leq$ resulta ser un (clase) orden parcial. El Corolario 9.55 nos dice que el Axioma de Elección implica que éste es un (clase) orden lineal. En seguida demostraremos la implicación recíproca.

Lema 10.1 *Para cualquier conjunto X, existe un conjunto de números ordinales A tal que $\alpha \in A$ si y sólo si $|\alpha| \leq |X|$.*

DEMOSTRACIÓN:

Sea X un conjunto y sea

$$\mathcal{X} = \{R \subseteq X \times X : (dom\, R, R) \text{ es un conjunto bien ordenado}\}.$$

Para cada $R \in \mathcal{X}$, existe un único número ordinal α tal que

$$\|(dom\, R, R)\| = \alpha.$$

Defina

$$\mathbf{F}(x) = \begin{cases} \|(dom\, R, R)\|, & \text{si } x = R \in \mathcal{X} \\ \emptyset, & \text{en otro caso.} \end{cases}$$

Entonces $\mathbf{F}$ es una (clase) función, y se sigue del Axioma Esquema de Reemplazo que $\mathbf{F}(\mathcal{X})$ es un conjunto. Claramente,

$$\{\alpha \in \mathbf{Ord} : |\alpha| \leq |X|\} \supseteq \mathbf{F}(\mathcal{X}).$$

Por otro lado, si $|\beta| \leq |X|$, entonces existe $Y \subseteq X$ tal que $|\beta| = |Y|$. Sea $g : Y \to \beta$ una biyección y defina una relación R como sigue:

$$R = \{(u, v) : u, v \in Y \quad \wedge \quad g(u) \leq g(v)\}.$$

Obviamente $dom\, R = Y$, (Y, R) es un conjunto bien ordenado y $\|(Y, R)\| = \beta$; así, $\mathbf{F}(R) = \beta$. Consecuentemente,

$$\mathbf{F}(\mathcal{X}) = \{\alpha \in \mathbf{Ord} : |\alpha| \leq |X|\}. \quad \blacksquare$$

Definición 10.2 Para cualquier conjunto X, denotamos

$$\Gamma(X) = \{\alpha \in \mathbf{Ord} : |\alpha| \leq |X|\}.$$

A $\Gamma(X)$ se le llama *función de Hartog.*

$\Gamma(X)$ es un conjunto de números ordinales, probaremos que $\Gamma(X)$ es de hecho un número ordinal.

Proposición 10.3 *Para cada X, $\Gamma(X)$ es un número ordinal.*

DEMOSTRACIÓN:

Sea X un conjunto. Ya que $\Gamma(X)$ es un conjunto de números ordinales, para mostrar que $\Gamma(X)$ es un número ordinal es suficiente demostrar que es transitivo. Supóngase que $\alpha \in \Gamma(X)$ y que $\beta \in \alpha$. Entonces $|\alpha| \leq |X|$ y $\beta \subseteq \alpha$; por lo tanto, $|\beta| \leq |X|$, así $\beta \in \Gamma(X)$. ■

Ahora procederemos a mostrar que la tricotomía del orden entre números cardinales implica el Teorema del Buen Orden.

Teorema 10.4 (Hartog) *El Axioma de Elección es equivalente a la afirmación de que cualesquiera dos números cardinales son $\leq$-comparables.*

DEMOSTRACIÓN:

Nos resta probar la suficiencia (ver Corolario 9.55). Supongamos que cualesquiera dos números cardinales son comparables. Sea X un conjunto. Por hipótesis, o bien $|X| \leq |\Gamma(X)|$ o $|\Gamma(X)| \leq |X|$. Puesto que $\Gamma(X)$ es un número ordinal, si $|\Gamma(X)| \leq |X|$, entonces $\Gamma(X) \in \Gamma(X)$; que es imposible (pues ningún número ordinal es elemento de sí mismo). Por lo tanto, se debe tener $|X| \leq |\Gamma(X)|$; y esto claramente implica que X puede ser bien ordenado. ■

Existen otras versiones de la tricotomía que también son equivalentes al Axioma de Elección. Algunas de esas versiones pueden encontrarse en [RR, pag. 21].

Si el Axioma de Elección no se usa, la aritmética cardinal pierde la simplicidad de la aritmética cardinal con el Axioma de Elección (ver Sección 9.7). Muchas de las fórmulas dejan de ser válidas y aquellas que se mantienen se vuelven difíciles de establecer. En lo que resta de esta sección presentamos algunos resultados típicos de la relación entre el Axioma de Elección y la aritmética de cardinales.

Para cualquier cardinal infinito κ, el *número de Hartog de* κ es $\hbar(A)$, donde $|A| = \kappa$. En vista del Lema 9.57, $\hbar(A)$ es un aleph que denotaremos por $\aleph(\kappa)$. Observemos que $\aleph(\kappa)$ tiene la propiedad de ser el mínimo aleph tal que $\aleph(\kappa) \not\leq \kappa$.

Lema 10.5 *Si κ es un cardinal infinito, si $\aleph$ es un aleph y si*

$$\kappa + \aleph = \kappa \cdot \aleph, \tag{10.1.1}$$

entonces, o bien $\kappa \geq \aleph$ o $\kappa \leq \aleph$. En particular, si

$$\kappa + \aleph(\kappa) = \kappa \cdot \aleph(\kappa), \tag{10.1.2}$$

entonces κ es un aleph.

DEMOSTRACIÓN:

Sea K un conjunto tal que $\kappa = |K|$, y sea W un conjunto bien ordenado tal que $\aleph = |W|$. Por la ecuación (10.1.1), existen subconjuntos ajenos K_1 y W_1 de $K \times W$ tales que $K \times W = K_1 \cup W_1$ y $|K_1| = \kappa$, $|W_1| = \aleph$. Ahora bien, si existe $k \in K$ tal que $(k, w) \in K_1$ para cualquier $w \in W$, entonces $\kappa \geq \aleph$ puesto que $K_1 \supseteq \{(k, w) : w \in W\}$. Si por el contrario, cada $\{k\} \times W \nsubseteq K_1$, entonces, para cada $k \in K$, podemos tomar el mínimo elemento w_k de W tal que $(k, w_k) \in W_1$. Resulta ahora que $\kappa \leq \aleph$, puesto que $\{(k, w_k) : k \in K\} \subseteq W_1$.

En el caso particular de la ecuación (10.1.2), $\kappa \geq \aleph(\kappa)$ es imposible, y $\kappa \leq \aleph(\kappa)$ implica que κ es un aleph. ■

Usaremos el lema anterior para establecer los siguientes resultados.

Teorema 10.6 (Tarski) *El Axioma de Elección es equivalente a que cualesquiera dos números cardinales κ y λ cumplen*

$$\kappa + \lambda = \kappa \cdot \lambda.$$

DEMOSTRACIÓN:

Mostraremos que bajo las hipótesis del teorema cualquier cardinal infinito es un aleph. Sea κ un cardinal infinito, por el Lema 10.5 se sigue que $\kappa \leq \aleph(\kappa)$, lo cual dice que κ es un aleph. ■

Teorema 10.7 (Tarski) *El Axioma de Elección es equivalente a la siguiente proposición: Para cualquier número cardinal infinito κ, se tiene que $\kappa^2 = \kappa$.*

DEMOSTRACIÓN:

Empleando la misma técnica del teorema anterior, es suficiente mostrar que

$$\kappa + \aleph(\kappa) = \kappa \cdot \aleph(\kappa).$$

Como $\kappa + \aleph(\kappa) \leq \kappa \cdot \aleph(\kappa)$, debemos probar únicamente que $\kappa + \aleph(\kappa) \geq \kappa \cdot \aleph(\kappa)$. Esto se demuestre como sigue:

$$\kappa + \aleph(\kappa) = (\kappa + \aleph(\kappa))^2 = \kappa^2 + 2\kappa \cdot \aleph(\kappa) + \aleph(\kappa)^2 \geq \kappa \cdot \aleph(\kappa). \quad ■$$

El siguiente resultado es de naturaleza similar.

Teorema 10.8 (Tarski) *El Axioma de Elección es equivalente a la siguiente proposición: $\kappa^2 = \lambda^2$ implica $\kappa = \lambda$, para cualesquiera números cardinales infinitos κ y λ.*

DEMOSTRACIÓN:

Nuevamente mostraremos que cualquier número cardinal es un aleph. Sea κ un cardinal infinito y sea $\lambda = \kappa^{\aleph_0}$. Basta demostrar que λ es un aleph. Primero note que $\lambda^2 = \lambda$ puesto que

$$\lambda^2 = \left(\kappa^{\aleph_0}\right)^2 = \kappa^{2\aleph_0} = \kappa^{\aleph_0} = \lambda.$$

Así tenemos que

$$(\lambda \cdot \aleph(\lambda))^2 = \lambda \cdot \aleph(\lambda).$$

Ahora mostremos que

$$(\lambda + \aleph(\lambda))^2 = \lambda \cdot \aleph(\lambda).$$

Por un lado tenemos:

$$(\lambda + \aleph(\lambda))^2 = \lambda^2 + 2\lambda \cdot \aleph(\lambda) + \aleph(\lambda)^2 \geq \lambda \cdot \aleph(\lambda),$$

y por otro lado,

$$\begin{aligned}(\lambda + \aleph(\lambda))^2 &= \lambda^2 + 2 \cdot \lambda \cdot \aleph(\lambda) + \aleph(\lambda)^2 \\ &= \lambda + \aleph(\lambda) + \lambda \cdot \aleph(\lambda) \\ &\leq \lambda \cdot \aleph(\lambda) + \lambda + \aleph(\lambda) \\ &= \lambda \cdot 2\aleph(\lambda) = \lambda \cdot \aleph(\lambda),\end{aligned}$$

y consecuentemente λ es un aleph. ■

Ejercicios 10.1

1. Muestre que $\Gamma(X)$ es igual al número de Hartog de X.

2. (a) Demuestre que el Axioma de Elección es equivalente a la siguiente proposición: Para cualesquiera cardinales κ y λ, si $2\kappa < \kappa + \lambda$ entonces $\kappa < \lambda$.

   (b) Demuestre que la proposición "si $2\kappa > \kappa + \lambda$, entonces $\kappa > \lambda$" puede demostrarse sin el Axioma de Elección.

3. Demuestre que las siguientes proposiciones son equivalentes al Axioma de Elección.

(a) Para cualesquiera números cardinales, κ, λ y μ, la inecuación $\kappa + \mu < \lambda + \mu$ implica $\kappa < \lambda$.

(b) Para cualesquiera números cardinales, κ, λ y μ, la inecuación $\kappa \cdot \mu < \lambda \cdot \mu$ implica $\kappa < \lambda$.

(c) Para cualquier número cardinal κ, se tiene $2 \cdot \kappa = \kappa$.

10.2 Sumas y Productos Infinitos

En esta sección procederemos a generalizar la suma de números cardinales.

Definición 10.9 Sea $\{A_i\}_{i\in I}$ una familia de conjuntos ajenos por pares, y sea $|A_i| = \kappa_i$ para cada $i \in I$. Definimos la *suma de* $\{\kappa_i\}_{i\in I}$ por

$$\sum_{i\in I} \kappa_i = \left|\bigcup_{i\in I} A_i\right|.$$

La definición de $\sum_{i\in I} \kappa_i$ usa conjuntos particulares A_i ($i \in I$). En el caso finito, cuando $I = \{1, 2\}$, y $\kappa_1 + \kappa_2 = |A_1 \cup A_2|$, demostramos que la elección de A_1 y A_2 es irrelevante. Para sumas infinitas, se necesita el Axioma de Elección para demostrar el lema correspondiente. Esta y otras razones nos llevan a *asumir el Axioma de Elección de ahora en adelante sin decirlo explícitamente.*

Lema 10.10 *Si* $\{A_i\}_{i\in I}$ *y* $\{A'_i\}_{i\in I}$ *son familias de conjuntos ajenos por pares tales que* $|A_i| = |A'_i|$ *para todo* $i \in I$*, entonces*

$$\left|\bigcup_{i\in I} A_i\right| = \left|\bigcup_{i\in I} A'_i\right|.$$

Demostración:

Para cada $i \in I$, seleccione una biyección $f_i : A_i \to A'_i$. Entonces $f = \bigcup_{i\in I} f_i$ es una biyección entre $\bigcup_{i\in I} A_i$ y $\bigcup_{i\in I} A'_i$. ■

Este lema hace que la definición de $\sum_{i\in I} \kappa_i$ sea legítima. Como las uniones infinitas de conjuntos satisfacen las ley asociativa, se sigue que las sumas infinitas de cardinales son también asociativas. La operación $\sum$ tiene otras propiedades razonables: Si $\kappa_i \leq \lambda_i$ para cada $i \in I$, entonces $\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i$. Sin embargo, si $\kappa_i < \lambda_i$ para cada $i \in I$, no necesariamente es cierto que $\sum_{i\in I} \kappa_i < \sum_{i\in I} \lambda_i$.

Si los sumandos son iguales, entonces también se tiene lo siguiente como en el caso finito. Si $\kappa = \kappa_i$ para cada $i \in \lambda$, entonces

$$\sum_{i\in\lambda} \kappa_i = \underbrace{\kappa + \kappa + \cdots}_{\lambda \text{ veces}} = \kappa \cdot \lambda.$$

No es muy difícil evaluar sumas infinitas. Por ejemplo, consideremos

$$1 + 2 + 3 + \cdots + n + \cdots \qquad (n \in \mathbf{N}).$$

Es fácil ver que esta suma, $\sum_{n\in\mathbf{N}} n$, es igual a $\aleph_0$. Este hecho se deduce del siguiente teorema general.

Teorema 10.11 *Sea λ un cardinal infinito, sea κ_α un número cardinal no nulo para cada $\alpha < \lambda$, y sea $\kappa = \sup\{\kappa_a : \alpha < \lambda\}$. Entonces*

$$\sum_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \kappa = \lambda \cdot \sup\{\kappa_\alpha : \alpha < \lambda\}.$$

Demostración:

Por un lado, $\kappa_\alpha \leq \kappa$ para cada $\alpha < \lambda$. Entonces

$$\sum_{\alpha<\lambda} \kappa_\alpha \leq \sum_{\alpha<\lambda} \kappa = \kappa \cdot \lambda.$$

Por otro lado, note que $\lambda = \sum_{\alpha<\lambda} 1 \leq \sum_{\alpha<\lambda} \kappa_\alpha$. También tenemos $\kappa \leq \sum_{\alpha<\lambda} \kappa_\alpha$; en efecto, puesto que κ es el supremo de $\{\kappa_\alpha\}_{\alpha<\lambda}$, cualquier γ menor que κ es menor que algún κ_α, y $\kappa_\alpha \leq \sum_{\alpha<\lambda} \kappa_\alpha$; por tanto, $\kappa \leq \sum_{\alpha<\lambda} \kappa_\alpha$. Ahora ya que κ y λ son menores o iguales que $\sum_{\alpha<\lambda} \kappa_\alpha$, se sigue que $\kappa \cdot \lambda$, que es el máximo de los dos, es también menor o igual que $\sum_{\alpha<\lambda} \kappa_\alpha$. Finalmente, usando el Teorema de Cantor-Schröder-Bernstein se concluye el teorema. ■

Corolario 10.12 *Si κ_i $(i \in I)$ son números cardinales y $|I| \leq \sup\{\kappa_i : i \in I\}$, entonces*

$$\sum_{i\in I} \kappa_i = \sup\{\kappa_i : i \in I\}.$$

En particular, la igualdad se satisface si todos los κ_i son mutuamente distintos.

El producto de dos números cardinales κ_1 y κ_2 es el número cardinal del producto cartesiano $A_1 \times A_2$, donde A_1, A_2 son conjuntos arbitrarios tales que $|A_1| = \kappa_1$ y $|A_2| = \kappa_2$. Esto se generaliza como sigue.

Definición 10.13 Sea $\{A_i\}_{i\in I}$ una familia de conjuntos tales que $|A_i| = \kappa_i$ para cada $i \in I$. Se define el *producto de* $\{\kappa_i\}_{i\in I}$ por

$$\prod_{i\in I} \kappa_i = \left|\prod_{i\in I} A_i\right|.$$

Se usa el mismo símbolo para el producto de cardinales (el del lado izquierdo) que para el producto cartesiano de la familia indizada $\{A_i\}_{i\in I}$ (el del lado derecho). Según el contexto, será claro el significado del símbolo $\prod$.

Nuevamente, la definición de $\prod_{i\in I} \kappa_i$ no depende de los conjuntos particulares A_i.

Lema 10.14 *Si* $\{A_i\}_{i\in I}$ *y* $\{A'_i\}_{i\in I}$ *son tales que* $|A_i| = |A'_i|$ *para todo* $i \in I$, *entonces*

$$\left|\prod_{i\in I} A_i\right| = \left|\prod_{i\in I} A'_i\right|.$$

Demostración:

Para cada $i \in I$, elíjase una biyección $f_i : A_i \to A'_i$. Sea

$$f : \prod_{i\in I} A_i \to \prod_{i\in I} A'_i$$

la función cuya i-ésima función coordenada es f_i, es decir, $f = (f_i)_{i\in I}$. Entonces f es una biyección. ■

Los productos infinitos también tienen muchas propiedades esperadas; por ejemplo, si algún κ_i es igual a 0, entonces $\prod_{i\in I} \kappa_i = 0$. El producto también satisface la ley asociativa. Otra propiedad simple es que si $\kappa_i \le \lambda_i$ para todo $i \in I$, entonces $\prod_{i\in I} \kappa_i \le \prod_{i\in I} \lambda_i$. Si todos los factores κ_i son el mismo, digamos κ, entonces

$$\prod_{i\in\lambda} \kappa_i = \underbrace{\kappa \cdot \kappa \cdot \cdots}_{\lambda \text{ veces}} = \kappa^\lambda .$$

Las siguientes reglas que involucran exponenciación son generalizaciones del caso finito:

$$\left(\prod_{i\in I} \kappa_i\right)^\lambda = \prod_{i\in I} (\kappa_i)^\lambda,$$

$$\prod_{i\in I} (\kappa^{\lambda_i}) = \kappa^{\sum_{i\in I} \lambda_i}.$$

Los productos infinitos de números cardinales son más difíciles de evaluar que las sumas infinitas de números cardinales. Pueden demostrarse algunas reglas simples en algunos casos especiales; por ejemplo, cuando se evalúa el producto $\prod_{\alpha<\lambda}\kappa_\alpha$ de una sucesión creciente $(\kappa_\alpha)_{\alpha<\lambda}$ de números cardinales. Consideremos el siguiente caso muy especial:

$$\kappa = 1\cdot 2\cdot 3\cdot\cdots = \prod_{n=1}^{\infty} n.$$

Primero note que

$$\kappa = \prod_{n=1}^{\infty} n \leq \prod_{n=1}^{\infty} \aleph_0 = \aleph_0^{\aleph_0} = 2^{\aleph_0}.$$

Recíprocamente,

$$2^{\aleph_0} \leq \prod_{n=1}^{\infty} 2 \leq \prod_{n=2}^{\infty} n = \prod_{n=1}^{\infty} n = \kappa$$

y concluimos que $1\cdot 2\cdot 3\cdot\cdots = 2^{\aleph_0}$. En general tenemos el siguiente teorema.

Teorema 10.15 *Si λ es un cardinal infinito, $(\kappa_\alpha)_{\alpha<\lambda}$ es una sucesión no decreciente de cardinales no nulos y $\kappa = \sup\{\kappa_\alpha : \alpha<\lambda\}$, entonces*

$$\prod_{\alpha<\lambda}\kappa_\alpha = \kappa^\lambda.$$

Demostración:

Como $\kappa_\alpha \leq \kappa$ para cada $\alpha<\lambda$, tenemos que

$$\prod_{\alpha<\lambda}\kappa_\alpha \leq \prod_{\alpha<\lambda}\kappa = \kappa^\lambda$$

Para probar que $\kappa^\lambda \leq \prod_{\alpha<\lambda}\kappa_\alpha$, consideremos una partición de λ en λ conjuntos A_α de cardinalidad λ:

$$\lambda = \bigcup_{\alpha<\lambda} A_\alpha$$

(ver Ejercicio 10.2.7). Como cada A_β debe ser no acotado en λ y dado que el producto de cardinales no nulos es mayor o igual que cada factor, tenemos que

$$\prod_{\alpha\in A_\beta}\kappa_\alpha \geq \sup\{\kappa_\alpha : \alpha\in A_\beta\} = \kappa,$$

para cada $\alpha < \lambda$. Usando la asociatividad del producto infinito obtenemos (ver Ejercicio 10.2.8)

$$\prod_{\alpha<\lambda} \kappa_\alpha = \prod_{\beta<\lambda} \left(\prod_{\alpha\in A_\beta} \kappa_\beta \right) \geq \prod_{\beta<\lambda} \kappa = \kappa^\lambda. \quad \blacksquare$$

Ahora demostraremos un importante teorema, el cual puede emplearse para derivar varias inecuaciones en aritmética cardinal.

Teorema 10.16 (König) *Si κ_i y λ_i para $i \in I$, son números cardinales y si $\kappa_i < \lambda_i$ para cada $i \in I$, entonces*

$$\sum_{i\in I} \kappa_i < \prod_{i\in I} \lambda_i.$$

Demostración:

Mostraremos que $\sum_{i\in I} \kappa_i \not\geq \prod_{i\in I} \lambda_i$. Sea $\{A_i\}_{i\in I}$ una familia de conjuntos tales que $|A_i| = \lambda_i$ para cada $i \in I$. Es suficiente mostrar que si $\{B_i\}_{i\in I}$ es una familia de subconjuntos de $A = \prod_{i\in I} A_i$ tal que $|B_i| \leq \kappa_i$ para cada $i \in I$, entonces $\bigcup_{i\in I} B_i \neq A$.

Para cada $i \in I$, consideremos las proyección de B_i sobre el i-ésimo factor $S_i = p_i(B_i)$. Como $|B_i| < |A_i|$, tenemos que $S_i \subset A_i$. Ahora sea $x = (x_i)_{i\in I} \in A$ un elemento tal que $x_i \notin S_i$. Obviamente, x no pertenece a cualquier B_i $(i \in I)$ y así $\bigcup_{i\in I} B_i \neq A$. $\blacksquare$

El Teorema de König es una generalización del Teorema de Cantor el cual asegura que $2^\kappa > \kappa$. Si expresamos κ como una suma infinita

$$\kappa = \underbrace{1 + 1 + 1 + \cdots}_{\kappa \text{ veces}}$$

y 2^κ como un producto infinito

$$2^\kappa = \underbrace{2 \cdot 2 \cdot 2 \cdots}_{\kappa \text{ veces}},$$

entonces el Teorema de König es aplicable ya que $1 < 2$, y obtenemos

$$\kappa = \sum_{i\in\kappa} 1 < \prod_{i\in\kappa} 2 = 2^\kappa.$$

Ejercicios 10.2

1. Demuestre que si $\{J_i\}_{i\in I}$ es una familia de conjunto ajenos por pares, $J = \bigcup_{i\in I} J$ y κ_j $(j \in J)$ son números cardinales, entonces

$$\sum_{i\in I}(\sum_{j\in J_i} \kappa_j) = \sum_{j\in J} \kappa_j$$

   (*asociatividad* de $\sum$).

2. Pruebe que si $\kappa_i \leq \lambda_i$ para cada $i \in I$, entonces

$$\sum_{i\in I} \kappa_i \leq \sum_{i\in I} \lambda_i.$$

3. Encuentre cardinales κ_n y λ_n $(n \in \mathbf{N})$ tales que $\kappa_n < \lambda_n$ para todo $n \in \mathbf{N}$, pero $\sum_{n=0}^{\infty} \kappa_n = \sum_{n=0}^{\infty} \lambda_n$.

4. Pruebe que $\kappa + \kappa + \cdots$ (λ veces) es igual a $\lambda \cdot \kappa$.

5. Demuestre la ley distributiva

$$\lambda \cdot \left(\sum_{i\in I} \kappa_i\right) = \sum_{i\in I} (\lambda \cdot \kappa_i).$$

6. Pruebe que

$$\left|\bigcup_{i\in I} A_i\right| \leq \sum_{i\in I} |A_i| .$$

7. Demuestre que para cualquier α, $\aleph_\alpha$ puede representarse como la unión de una familia de cardinalidad $\aleph_\alpha$, formada por subconjuntos de cardinalidad $\aleph_\alpha$. (Sugerencia: ver Teorema 9.60.)

8. Demuestre que si $\{J_i\}_{i\in I}$ es una familia ajena por pares, $J = \bigcup_{i\in I} J_i$ y κ_i son números cardinales, entonces

$$\prod_{i\in I}\left(\prod_{j\in J_i} \kappa_j\right) = \prod_{j\in J} \kappa_j$$

   (*asociatividad* de $\prod$).

9. Pruebe que si $\kappa_i \leq \lambda_i$ para $i \in I$, entonces
$$\prod_{i\in I} \kappa_i \leq \prod_{i\in I} \lambda_i.$$

10. Encuentre cardinales κ_n y λ_n ($n \in \mathbf{N}$) tales que $\kappa_n < \lambda_n$, pero $\prod_{n=0}^{\infty} \kappa_n = \prod_{n=0}^{\infty} \lambda_n$.

11. Pruebe que $\kappa \cdot \kappa \cdot \cdots$ (λ veces) es igual a κ^{λ}.

12. Demuestre la fórmula
$$\left(\prod_{i\in I} \kappa_i\right)^{\lambda} = \prod_{i\in I} (\kappa_i^{\lambda}).$$

13. Demuestre la fórmula
$$\prod_{i\in I} (\kappa^{\lambda_i}) = \kappa^{\sum_{i\in I} \lambda_i}.$$

14. Demuestre que si $1 < \kappa_i \leq \lambda_i$ para cada $i \in I$, entonces $\sum_{i\in I} \kappa_i \leq \prod_{i\in I} \lambda_i$.

15. Demuestre que la cardinalidad de
$$\prod_{0<\alpha<\omega_1} \alpha$$
es igual a $2^{\aleph_1}$.

16. Demuestre que:
    (a) $\prod_{n<\omega} \aleph_n = \aleph_{\omega}^{\aleph_0}$.
    (b) $\prod_{\alpha<\omega+\omega} \aleph_\alpha = \aleph_{\omega+\omega}^{\aleph_0}$.

10.3 Cardinales Regulares y Singulares

Sea $(\alpha_v)_{v<\theta}$ una sucesión transfinita de números ordinales de longitud θ. Diremos que la sucesión $(\alpha_v)_{v<\theta}$ es *creciente* si $\alpha_v < \alpha_\mu$ siempre que $\nu < \mu < \theta$. Si θ es un ordinal límite y si $(\alpha_v)_{v<\theta}$ es una sucesión creciente de ordinales, definimos
$$\alpha = \lim_{v\to\theta} \alpha_v = \sup\{\alpha_v : v < \theta\}$$
y llamamos a α el *límite* de la sucesión creciente.

Definición 10.17 Un cardinal infinito κ se llama *singular* si existe una sucesión transfinita creciente $(\alpha_\nu)_{\nu<\theta}$ de ordinales $\alpha_\nu < \kappa$ cuya longitud θ es un ordinal límite menor que κ, y

$$\kappa = \lim_{\nu\to\theta} \alpha_\nu.$$

Un cardinal infinito que no es singular se llama *regular.*

Por ejemplo, un cardinal singular es $\aleph_\omega$: pues

$$\aleph_\omega = \lim_{n\to\omega} \aleph_n,$$

en donde $\omega < \aleph_\omega$ y $\aleph_n < \aleph_{n+1}$ para cada $n < \omega$.

Similarmente, los cardinales $\aleph_{\omega+\omega}$, $\aleph_{\omega\cdot\omega}$, $\aleph_{\omega_1}$ son singulares: ya que

$$\aleph_{\omega+\omega} = \lim_{n\to\omega} \aleph_{\omega+n},$$

$$\aleph_{\omega\cdot\omega} = \lim_{n\to\omega} \aleph_{\omega\cdot n},$$

$$\aleph_{\omega_1} = \lim_{\alpha\to\omega_1} \aleph_\alpha.$$

Por otro lado, $\aleph_0$ es un cardinal regular. El siguiente lema nos proporciona una caracterización de los cardinales singulares.

Lema 10.18 *Un cardinal infinito κ es singular si y sólo si es igual a la suma de menos que κ cardinales menores: $\kappa = \sum_{\iota\in I} \kappa_i$, donde $|I| < \kappa$ y $\kappa_i < \kappa$ para cada $i \in I$.*

Demostración:

$\Rightarrow$] Si κ es singular, entonces existe una sucesión transfinita creciente tal que $\kappa = \lim_{\nu\to\theta} \alpha_\nu$, donde $\theta < \kappa$ y $\alpha_\nu < \kappa$ para todo $\nu < \theta$. Puesto que todo ordinal es igual al conjunto de todos los ordinales menores, puede probarse que

$$\kappa = \bigcup_{\nu<\theta} \alpha_\nu = \bigcup_{\nu<\theta} \left(\alpha_\nu - \bigcup_{\xi<\nu} \alpha_\xi \right).$$

Si hacemos $A_\nu = \alpha_\nu - \bigcup_{\xi<\nu} \alpha_\xi$, entonces $(A_\nu)_{v<\theta}$ es una sucesión de menos que κ conjuntos de cardinalidad $\kappa_\nu = |A_\nu| = \left|\nu - \bigcup_{\xi<\nu} \alpha_\xi\right| \leq |\alpha_\nu| < \kappa$, y dado que los conjuntos A_ν son ajenos por pares, esto muestra que

$$\kappa = \sum_{\nu<\theta} \kappa_\nu.$$

$\Leftarrow$] Supongamos que $\kappa = \sum_{\alpha<\lambda} \kappa_\alpha$, donde λ es un cardinal menor que κ y para todo $\alpha < \lambda$ se tiene que $\kappa_\alpha < \kappa$. Empleando el Teorema 10.11,

$$\kappa = \sum_{\alpha<\lambda} \kappa_\alpha = \lambda \cdot \sup\{\kappa_\alpha : \alpha < \lambda\}.$$

Como $\lambda < \kappa$, necesariamente tenemos que $\kappa = \sup\{\kappa_\alpha : \alpha < \lambda\}$; con lo cual, el rango de la sucesión transfinita $(\kappa_\alpha)_{\alpha<\lambda}$ tiene supremo igual a κ. Además, como $\kappa_\alpha < \kappa$ para cada $\alpha < \lambda$, podemos hallar, por inducción transfinita, una subsucesión creciente con límite κ. Claramente la longitud de la subsucesión que se obtiene es θ. Por lo tanto, κ es un cardinal singular. ■

Definición 10.19 Un cardinal infinito $\aleph_\alpha$ se llama *cardinal sucesor* si su índice α es un ordinal sucesor, es decir, $\aleph_\alpha = \aleph_{\beta+1}$ para algún β. Si α es un ordinal límite, entonces $\aleph_\alpha$ se llama *cardinal límite.*

Es valioso observar que si $\alpha > 0$ es un ordinal límite, entonces $\aleph_\alpha$ es el límite de la sucesión $(\aleph_\beta)_{\beta<\alpha}$. También tenemos el siguiente teorema que nos proporciona información a cerca de los cardinales sucesores.

Teorema 10.20 *Cualquier cardinal sucesor $\aleph_{\alpha+1}$ es un cardinal regular.*

Demostración:

Supongamos lo contrario, es decir, supongamos que existe un cardinal sucesor $\aleph_{\alpha+1}$ que puede expresarse como suma de una cantidad menor de cardinales menores:

$$\aleph_{\alpha+1} = \sum_{i\in I} \kappa_i,$$

donde $|I| < \aleph_{\alpha+1}$, y $\kappa_i < \aleph_{\alpha+1}$ para cada $i \in I$. Entonces $|I| \leq \aleph_\alpha$ y $\kappa_i \leq \aleph_\alpha$ para cada $i \in I$; por lo que se obtiene

$$\aleph_{\alpha+1} = \sum_{i\in I} \kappa_i \leq \sum_{i\in I} \aleph_\alpha = \aleph_\alpha \cdot |I| \leq \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha.$$

Esta es una contradicción que establece el teorema. ■

Una conclusión del teorema precedente es que todo cardinal singular es un cardinal límite. Podemos demostrar más.

Proposición 10.21 *Hay cardinales singulares arbitrariamente grandes.*

DEMOSTRACIÓN:

Sea $\aleph_\alpha$ un cardinal arbitrario. Considere la sucesión

$$\aleph_\alpha,\ \aleph_{\alpha+1},\ \aleph_{\alpha+2},\ \ldots,\ \aleph_{\alpha+n},\ \ldots \quad (n < \omega).$$

Entonces

$$\aleph_{\alpha+\omega} = \lim_{n\to\omega} \aleph_{\alpha+n},$$

y por lo tanto, $\aleph_{\alpha+\omega}$ es un cardinal singular mayor que $\aleph_\alpha$. ■

La regularidad de cardinales fue investigada por Hausdorff quien se preguntó sobre la existencia de cardinales regulares límites. Analicemos un poco este asunto: Supóngase que $\aleph_\alpha$ es uno de tales cardinales. Puesto que α es un ordinal límite, tenemos que

$$\aleph_\alpha = \lim_{\beta\to\alpha} \aleph_\beta;$$

es decir, $\aleph_\alpha$ es el límite de una sucesión creciente de longitud α. Ya que $\aleph_\alpha$, es regular, necesariamente tenemos que $\alpha \geq \aleph_\alpha$, lo cual, aunado con $\alpha \leq \aleph_\alpha$, nos proporciona

$$\alpha = \aleph_\alpha. \tag{10.3.1}$$

Esta propiedad sugiere que $\aleph_\alpha$ debe ser muy grande. Por otra parte, la condición (10.3.1) parece ser muy fuerte, sin embargo no lo es tanto.

Proposición 10.22 *Hay cardinales singulares $\aleph_\alpha$ arbitrariamente grandes - que tienen la propiedad $\alpha = \aleph_\alpha$.*

DEMOSTRACIÓN:

Sea $\aleph_\gamma$ un cardinal arbitrario. Consideremos la siguiente sucesión:

$$\begin{gathered}
\alpha_0 = \omega_\gamma \\
\alpha_1 = \omega_{\alpha_0} = \omega_{\omega_\gamma} \\
\alpha_2 = \omega_{\alpha_1} = \omega_{\omega_{\omega_\gamma}} \\
\cdots \\
\alpha_{n+1} = \omega_{\alpha_n} \\
\cdots
\end{gathered}$$

para todo $n < \omega$, y sea $\alpha = \lim_{n\to\omega} \alpha_n$. Es claro que la sucesión $(\aleph_{\alpha_n})_{n<\omega}$ tiene límite $\aleph_\alpha$. Pero entonces tenemos que

$$\aleph_\alpha = \lim_{n\to\omega} \aleph_\alpha = \lim_{n\to\omega} \alpha_{n+1} = \alpha.$$

Puesto que $\aleph_\alpha$ es el límite de una sucesión de cardinales menores de longitud ω, éste es singular. ■

Definición 10.23 Un cardinal no numerable $\aleph_\alpha$ que es a la vez un cardinal límite y regular es llamado *(débilmente) inaccesible.*

Es imposible demostrar a partir de los axiomas **ZFC** que los cardinales inaccesibles existen; en otras palabras, puede incluirse como un axioma adicional para la Teoría de Conjuntos que los cardinales inaccesibles existen.

Definición 10.24 Si α es un ordinal límite, entonces la *cofinalidad* de α, denotada por $cf(\alpha)$, es el mínimo número ordinal θ tal que α es el límite de una sucesión creciente de ordinales de longitud θ.

Note que $cf(\alpha)$ es un ordinal límite y que $cf(\alpha) \leq \alpha$. Así, $\aleph_\alpha$ es singular si $cf(\alpha) < \alpha$ y es regular si $cf(\alpha) = \alpha$.

Proposición 10.25 *Si un ordinal límite α no es un número cardinal, entonces $cf(\alpha) < \alpha$.*

Demostración:

Sea α un ordinal límite que no sea un número cardinal. Si hacemos $\kappa = |\alpha|$, entonces existe una función inyectiva de κ sobre α, o en otras palabras, existe una sucesión inyectiva $(\alpha_\nu)_{\nu<\kappa}$ de longitud κ tal que $\{\alpha_\nu : \nu < \kappa\} = \alpha$. Ahora podemos hallar (por inducción transfinita) una subsucesión que sea creciente y su límite sea α. Dado que la longitud de la subsucesión es a lo más κ, y puesto que $|\alpha| = \kappa < \alpha$ (pues α no es un número cardinal), concluimos que $cf(\alpha) < \alpha$. ■

Corolario 10.26 *Para cualquier ordinal límite α, $cf(\alpha) = \alpha$ si y sólo si α es un cardinal regular.*

Proposición 10.27 *Para cualquier ordinal límite α,*

$$cf(cf(\alpha)) = cf(\alpha).$$

Demostración:

Sea $\theta = cf(\alpha)$. Claramente, θ es un ordinal límite y $cf(\theta) \leq \theta$. Demostraremos que $cf(\theta)$ no es menor que θ. Si $\gamma = cf(\theta) < \theta$, entonces existe una sucesión creciente de ordinales $(\nu_\xi)_{\xi<\gamma}$ tal que su límite $\lim_{\xi\to\gamma} \nu_\xi = \theta$. Puesto que $\theta = cf(\alpha)$, existe una sucesión creciente $(\alpha_\nu)_{\nu<\theta}$ tal que $\lim_{\nu\to\theta} \alpha_\nu = \alpha$. Pero entonces la sucesión $(\alpha_{\nu_\xi})_{\xi<\gamma}$ tiene longitud γ, y $\lim_{\xi\to\gamma} \alpha_{\nu_\xi} = \alpha$. Como $\gamma < \theta$,

esto es una contradicción, ya que θ es la mínima longitud de una sucesión creciente con límite α. ■

Corolario 10.28 *Para cualquier ordinal límite α, $cf(\alpha)$ es un cardinal regular.*

Ejercicios 10.3

1. Demuestre que $cf(\aleph_\omega) = cf(\aleph_{\omega+\omega}) = \omega$.
2. Demuestre que $cf(\aleph_{\omega_1}) = \omega_1$, $cf(\aleph_{\omega_2}) = \omega_2$.
3. Sea α el número cardinal definido en la demostración de la Proposición 10.22. Demuestre que $cf(\alpha) = \omega$.
4. Muestre que $cf(\alpha)$ es el mínimo γ tal que α es la unión de γ conjuntos de cardinalidad menor que $|\alpha|$.
5. Sea $\aleph_\alpha$ un cardinal límite, $\alpha > 0$. Demuestre que hay una sucesión creciente de alephs de longitud $cf(\aleph_\alpha)$ con límite $\aleph_\alpha$.
6. Sea κ un cardinal infinito, y sea $\lambda < \kappa$ un cardinal regular infinito. Demuestre que existe una sucesión creciente $(\alpha_\nu)_{\nu<cf(\kappa)}$ de cardinales tales que $\lim_{\nu\to cf(\kappa)} \alpha_\nu = \kappa$ y $\lambda = cf(\alpha_\nu)$ para todo $\nu < cf(\kappa)$.

10.4 La Hipótesis Generalizada del Continuo

Mientras la suma y multiplicación de números cardinales es simple (debido al hecho de que $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$), la evaluación de la exponenciación de números cardinales es muy complicada. En la presente sección estudiaremos la operación $2^{\aleph_\alpha}$.

Por el Teorema de Cantor, $2^{\aleph\alpha} > \aleph_\alpha$; en otras palabras,

$$2^{\aleph_\alpha} \geq \aleph_{\alpha+1}. \tag{10.4.1}$$

No hay mucho que pueda demostrarse acerca de $2^{\aleph_\alpha}$, excepto la siguiente propiedad trivial:

$$2^{\aleph_\alpha} \leq 2^{\aleph_\beta} \quad \text{siempre que} \quad \alpha \leq \beta. \tag{10.4.2}$$

El siguiente hecho es una consecuencia del Teorema de König.

Proposición 10.29 *Para cualquier α,*

$$cf(2^{\aleph_\alpha}) > \aleph_\alpha. \tag{10.4.3}$$

Demostración:

Sea $\theta = cf(2^{\aleph_\alpha})$. θ es un cardinal. Así, $2^{\aleph_\alpha}$ es el límite de una sucesión creciente de longitud θ, y se sigue que

$$2^{\aleph_\alpha} = \sum_{\nu<\theta} \kappa_\nu,$$

donde cada κ_ν es un cardinal menor que $2^{\aleph_\alpha}$. Por el Teorema de König (donde se pone $\lambda_\nu = 2^{\aleph_\alpha}$ para todo $\nu < \theta$), tenemos que

$$\sum_{\nu<\theta} \kappa_\nu < \prod_{\nu<\theta} 2^{\aleph_\alpha}$$

y por lo tanto,

$$2^{\aleph_\alpha} < (2^{\aleph_\alpha})^\theta.$$

Ahora, si θ es menor o igual a $\aleph_\alpha$, se tendría que

$$2^{\aleph_\alpha} < (2^{\aleph_\alpha})^\theta = 2^{\aleph_\alpha \cdot \theta} = 2^{\aleph_\alpha},$$

que es una contradicción. ■

Una consecuencia de la Proposición 10.29 es que $2^{\aleph_0}$ no puede ser $\aleph_\omega$ (puesto que $cf(\aleph_\omega) = \aleph_0$), pero el lema no previene que $2^{\aleph_0}$ sea $\aleph_{\omega_1}$. Similarmente, $2^{\aleph_1}$ no puede ser $\aleph_{\omega_1}$, $\aleph_\omega$ o $\aleph_{\omega+\omega}$.

Las inecuaciones (10.4.1), (10.4.2) y (10.4.3) son las únicas propiedades que pueden demostrarse para la operación $2^{\aleph_\alpha}$ si el cardinal $\aleph_\alpha$ es regular. Si $\aleph_\alpha$ es singular, entonces varias reglas adicionales son conocidas.

Teorema 10.30 *Sea $\aleph_\alpha$ un cardinal singular. Supongamos que el valor de $2^{\aleph_\xi}$ es el mismo para todo $\xi < \alpha$, digamos $2^{\aleph_\xi} = \aleph_\beta$. Entonces también $2^{\aleph_\alpha} = \aleph_\beta$.*

Demostración:

Como $\aleph_\alpha$ es singular, existe por el Lema 10.18, una familia $\{\kappa_i\}_{i\in I}$ de cardinales tales que $\kappa_i < \aleph_\alpha$ para todo $i \in I$, con $|I| = \aleph_\gamma < \aleph_\alpha$, y $\aleph_\alpha = \sum_{i\in I} \kappa_i$. Por la suposición, tenemos que $2^{\kappa_i} = \aleph_\beta$ para todo $i \in I$, y que $2^{\aleph_\gamma} = \aleph_\beta$. Así,

$$\begin{aligned} 2^{\aleph_\alpha} &= 2^{\sum_{i\in I} \kappa_i} \\ &= \prod_{i\in I} 2^{\kappa_i} = \prod_{i\in I} \aleph_\beta \\ &= \aleph_\beta^{\aleph_\gamma} = (2^{\aleph_\gamma})^{\aleph_\gamma} \\ &= 2^{\aleph_\gamma} = \aleph_\beta. \quad ■ \end{aligned}$$

La generalización obvia de la Hipótesis del Continuo, la cual asegura que $2^{\aleph_0} = \aleph_1$, es la siguiente:

Hipótesis Generalizada del Continuo: *Para cualquier ordinal α, se tiene*

$$2^{\aleph_\alpha} = \aleph_{\alpha+1}. \tag{10.4.4}$$

En los trabajos de Gödel [G_2] de 1939 y Cohen [C_4] de 1963, se demostró que la Hipótesis Generalizada del Continuo es consistente e independiente de los axiomas **ZFC**. La Hipótesis Generalizada del Continuo es una proposición muy poderosa. En la siguiente sección veremos como simplifica la exponenciación de números cardinales. En la presente demostraremos que ella implica al propio Axioma de Elección; este teorema fue anunciado por A. Lindenbaun y A. Tarski en 1926, pero el primero en publicar una demostración fue Sierpiński en 1947. La demostración que presentaremos aquí es de E. Specker, publicada en 1954. Antes de formular dicho teorema es necesario hacer una observación sobre la Hipótesis Generalizada del Continuo. La forma en que fue expresada la Hipótesis Generalizada del Continuo, supone ya al Axioma de Elección, pero puede ser presentada sin hacer uso de este axioma (en particular, sin necesidad de suponer que cualquier número cardinal es un aleph). En efecto, la manera de presentar la Hipótesis Generalizada del Continuo (HGC) sin usar el Axioma de Elección es como sigue: *Para todos los cardinales infinitos κ, se tiene que*

$$si \;\; \kappa \leq \lambda \leq 2^\kappa, \; entonces \; \lambda = \kappa \;\; \text{o} \;\; \lambda = 2^\kappa. \tag{10.4.5}$$

En presencia del Axioma de Elección, (10.4.4) y (10.4.5) son obviamente equivalentes. Para demostrar el Teorema 10.32 emplearemos la segunda versión. Antes un lema.

Lema 10.31 *Si $\kappa \geq 5$, entonces $2^\kappa \not\leq \kappa^2$.*

Demostración:

Sean κ un cardinal infinito y X un conjunto con $|X| = \kappa$. Sea $\lambda = \hbar(X)$ el número de Hartog de X. Supongamos que $2^\kappa \leq \kappa^2$. Vamos a obtener una contradicción al construir una sucesión inyectiva de elementos de X de longitud λ.

Sea $f : \mathcal{P}(X) \to X \times X$ una función inyectiva, y para cualquier ordinal infinito α, sea $f_\alpha : \alpha \to \alpha \times \alpha$ una función inyectiva (ver demostración del Teorema 9.60). Vamos a construir una sucesión $(x_\alpha)_{\alpha<\lambda}$ como sigue: Seleccionemos x_0, x_1, x_2 x_3, x_4 en X de manera arbitraria. Si $n \geq 5$, sea

$C_n = \{x_0, \ldots, x_{n-1}\}$. Como

$$|\mathcal{P}(C_n)| = 2^n > n^2 = |C_n \times C_n|\,,$$

hay un subconjunto U de C_n tal que $f(U) \notin C_n \times C_n$. Sea U el primero de tales conjuntos (es decir, $U = \{x_{n_1}, \ldots, x_{n_k}\}$, donde $\{n_1, \ldots, n_k\}$ es el primero en un buen orden dado para la familia de subconjuntos finitos de $\mathbf{N}$). Si $f(U) = (x, y)$, entonces tomamos $x_n = x$ en el caso en que $x \notin C_n$ o tomamos $x_n = y$ si $x \in C_n$; en cualquier caso $x_n \notin C_n$. Para α un ordinal infinito con $\alpha < \lambda$, sea $C_\alpha = \{x_\xi : \xi < \alpha\}$. A partir de f y f_α, tenemos una función inyectiva $g : \alpha \to \mathcal{P}(X)$ tal que $g(\xi) = f^{-1}(x_\eta, x_\zeta)$, donde $(\eta, \zeta) = f_\alpha(\xi)$. Sea

$$U = \{x_\xi \in C_\alpha : x_\xi \notin g(\xi)\}\,,$$

y sea $(x, y) = f(U)$. Se sigue que $(x, y) \notin C_\alpha \times C_\alpha$, y así podemos hacer como antes $x_\alpha = x$ o $x_\alpha = y$. De esta manera tenemos la sucesión deseada. ■

Obsérvese que la elección de las funciones f_α o definir un buen orden en la familia de subconjuntos finitos de $\mathbf{N}$, no hace uso del Axioma de Elección. En el Teorema 9.60 se demuestra que las funciones f_α son definibles; por otra parte, el orden lexicográfico puede modificarse para obtener a un buen orden para $[\mathbf{N}]^{<\aleph_0}$.

Teorema 10.32 *La Hipótesis Generalizada del Continuo implica el Axioma de Elección.*

Demostración:

Sea κ un número cardinal. Asumiendo que la Hipótesis Generalizada del Continuo se cumple para cualquier λ, demostraremos que $\kappa^2 = \kappa$ (ver el segundo Teorema de Tarski). Primero, se afirma que

$$\kappa \leq 2 \cdot \kappa < 2^\kappa.$$

En efecto, dado que $\kappa \leq 2 \cdot \kappa$ y $2 \cdot \kappa \leq 2^\kappa$, y como $2 \cdot \kappa \leq \kappa^2$, tenemos que $2 \cdot \kappa \neq 2^\kappa$ por el Lema 10.31. Ahora se sigue de la Hipótesis Generalizada del Continuo que

$$2 \cdot \kappa = \kappa.$$

Con lo cual tenemos que $\kappa^2 < 2^\kappa$. Esto es porque

$$\kappa^2 \leq (2^\kappa)^2 = 2^{2 \cdot \kappa} = 2^\kappa,$$

y nuevamente por el Lema 10.31, $\kappa^2 \neq 2^\kappa$. Así tenemos que

$$\kappa \leq \kappa^2 < 2^\kappa,$$

que nos lleva a concluir: $\kappa = \kappa^2$. ■

Ejercicios 10.4

1. Usando el Axioma de Elección, demuestre la equivalencia entre las dos versiones de la Hipótesis Generalizada del Continuo.

2. Pruebe que si $2^{\aleph_0} > \aleph_\omega$, entonces $\aleph_\omega^{\aleph_0} = 2^{\aleph_0}$.

10.5 La HGC y los Números Cardinales

En esta sección mostraremos como la Hipótesis Generalizada del Continuo simplifica la exponenciación de números cardinales.

Lema 10.33 *Si $\alpha \leq \beta$, entonces $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$.*

DEMOSTRACIÓN:

Claramente, $2^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta}$. Como $\aleph_\alpha \leq 2^{\aleph_\beta}$, también tenemos

$$\aleph_\alpha^{\aleph_\beta} \leq (2^{\aleph_\alpha})^{\aleph_\beta} = 2^{\aleph_\alpha \cdot \aleph_\beta} = 2^{\aleph_\beta}. \quad \blacksquare$$

Lema 10.34 *Sean $\alpha \geq \beta$ y sea $\mathcal{S}$ la familia de todos los subconjuntos $X \subseteq \omega_\alpha$ tales que $|X| = \aleph_\beta$. Entonces $|\mathcal{S}| = \aleph_\alpha^{\aleph_\beta}$.*

DEMOSTRACIÓN:

Primero probaremos que $\aleph_\alpha^{\aleph_\beta} \leq |\mathcal{S}|$. Sea $\mathcal{S}'$ la familia de todos los subconjuntos $X \subseteq \omega_\beta \times \omega_\alpha$ tales que $|X| = \aleph_\beta$. Como $\aleph_\beta \cdot \aleph_\alpha = \aleph_\alpha$, tenemos que $|\mathcal{S}'| = |\mathcal{S}|$. Ahora, cualquier función $f : \omega_\beta \to \omega_\alpha$ es un miembro de la familia $\mathcal{S}'$ y, por tanto, $\omega_\alpha^{\omega_\beta} \subseteq \mathcal{S}'$. Por lo tanto, $\aleph_\alpha^{\aleph_\beta} \leq |\mathcal{S}|$.

Recíprocamente, si $X \in \mathcal{S}$, entonces existe una función f sobre ω_β tal que X es el rango de f. Tomemos una de tales f para cada $X \in \mathcal{S}$ y sea $f = F(X)$. Claramente, si $X \neq Y$ y $f = F(X)$, $g = F(Y)$, tenemos que $X = ran\, f$ y $Y = ran\, g$, así $f \neq g$. Esto nos muestra que $F : \mathcal{S} \to \omega_\alpha^{\omega_\beta}$ es una función inyectiva, y por lo tanto, $|\mathcal{S}| \leq \aleph_\alpha^{\aleph_\beta}$. $\blacksquare$

Ahora daremos una proposición para evaluar $\aleph_\alpha^{\aleph_\beta}$ para cardinales regulares $\aleph_\alpha$, bajo la suposición de la Hipótesis Generalizada del Continuo.

Teorema 10.35 *Suponiendo la Hipótesis Generalizada del Continuo, si $\aleph_\alpha$ es un cardinal regular, entonces*

$$\aleph_\alpha^{\aleph_\beta} = \begin{cases} \aleph_\alpha & si\ \beta < \alpha, \\ \aleph_{\beta+1} & si\ \ \beta \geq \alpha. \end{cases}$$

DEMOSTRACIÓN:

Si $\beta \geq \alpha$, entonces $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta} = \aleph_{\beta+1}$ por el Lema 10.33. Sea $\beta < \alpha$ y sea $\mathcal{B}$ la colección de todos los subconjuntos acotados de ω_α, esto es,

$$\mathcal{B} = \bigcup_{\delta<\omega_\alpha} \mathcal{P}(\delta).$$

Como $\aleph_\alpha$ es regular, se sigue que cualquier subconjunto $X \subseteq \omega_\alpha$ tal que $|X| = \aleph_\beta$ es un subconjunto acotado, y por el Lema 10.34, $\aleph_\alpha^{\aleph_\beta} \leq |\mathcal{B}|$. Así, es suficiente demostrar que $|\mathcal{B}| \leq \aleph_\alpha$.

Dado que $\mathcal{B} = \bigcup_{\delta<\omega_\alpha} \mathcal{P}(\delta)$, tenemos que

$$|\mathcal{B}| \leq \sum_{\delta<\omega_\alpha} 2^{|\delta|}.$$

Sin embargo, para cualquier cardinal $\aleph_\gamma < \aleph_\alpha$, se tiene que

$$2^{\aleph_\gamma} = \aleph_{\gamma+1} \leq \aleph_\alpha$$

y así $2^{|\delta|} \leq \aleph_\alpha$ para todo $\delta < \omega_\alpha$, y obtenemos

$$|\mathcal{B}| \leq \sum_{\delta<\omega_\alpha} 2^{|\delta|} \leq \sum_{\delta<\omega_\alpha} \aleph_\alpha = \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha. \ \blacksquare$$

Demostraremos una fórmula similar (pero un poco más complicada) para cardinales singulares $\aleph_\alpha$; primero es necesario generalizar la Proposición 10.29.

Lema 10.36 *Para cualquier cardinal $\kappa > 1$ y cualquier α,*

$$cf(\kappa^{\aleph_\alpha}) > \aleph_\alpha.$$

DEMOSTRACIÓN:

Es exactamente como la demostración de la Proposición 10.29, excepto que $2^{\aleph_\alpha}$ se reemplaza por $\kappa^{\aleph_\alpha}$. Los detalles los dejamos para el lector. ■

Teorema 10.37 *Suponiendo la Hipótesis Generalizada del Continuo, si $\aleph_\alpha$ es un cardinal singular, entonces*

$$\aleph_\alpha^{\aleph_\beta} = \begin{cases} \aleph_\alpha & si\ \aleph_\beta < cf(\aleph_\alpha), \\ \aleph_{\alpha+1} & si\ cf(\aleph_\alpha) \leq \aleph_\beta \leq \aleph_\alpha, \\ \aleph_{\beta+1} & si\ \aleph_\beta \geq \aleph_\alpha. \end{cases}$$

Demostración:

Si $\beta \geq \alpha$, entonces $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta} = \aleph_{\beta+1}$. Si $\aleph_\beta < cf(\aleph_\alpha)$, entonces cualquier subconjunto $X \subseteq \omega_\alpha$ tal que $|X| = \aleph_\beta$ es un subconjunto acotado, y tenemos que $\aleph_\alpha^{\aleph_\beta} = \aleph_\beta$ por el argumento empleado para cardinales regulares en el Teorema 10.35.

Así, supongamos que $cf(\aleph_\alpha) \leq \aleph_\beta \leq \aleph_\alpha$. Por una parte tenemos que

$$\aleph_\alpha \leq \aleph_\alpha^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\alpha} = 2^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

Por otra parte, dado que $\aleph_\alpha$ es singular, $cf(\aleph_\alpha^{\aleph_\beta}) \neq cf(\aleph_\alpha)$ y por lo tanto, $\aleph_\alpha^{\aleph_\beta} \neq \aleph_\alpha$. Así, necesariamente $\aleph_\alpha^{\aleph_\beta} = \aleph_{\alpha+1}$. ■

Dos consecuencias interesantes de los teoremas anteriores, de hecho de la Hipótesis Generalizada del Continuo, son las siguientes igualdades

$$\aleph_\alpha^{\aleph_\alpha} = \aleph_{\alpha+1} \tag{10.5.1}$$

y

$$\aleph_{\alpha+1}^{\aleph_\alpha} = \aleph_{\alpha+1}. \tag{10.5.2}$$

En seguida demostraremos que ambas (10.5.1) y (10.5.2) implican la Hipótesis Generalizada del Continuo.

Teorema 10.38 *La Hipótesis Generalizada del Continuo es equivalente a la proposición* $\aleph_\alpha^{\aleph_\alpha} = \aleph_{\alpha+1}$ *para cualquier número ordinal* α.

Demostración:

Sea α un número ordinal y supongamos que $\aleph_\alpha^{\aleph_\alpha} = \aleph_{\alpha+1}$. Entonces

$$\aleph_\alpha < 2^{\aleph_\alpha} \leq \aleph_\alpha^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

Sin embargo, no hay números cardinales entre $\aleph_\alpha$ y $\aleph_{\alpha+1}$, así debe ocurrir que

$$2^{\aleph_\alpha} = \aleph_{\alpha+1}.$$

La otra implicación se deja para el lector (ver Ejercicio 10.5.5). ■

Teorema 10.39 *La Hipótesis Generalizada del Continuo es equivalente a* $\aleph_{\alpha+1}^{\aleph_\alpha} = \aleph_{\alpha+1}$ *para cualquier número ordinal* α.

Si no suponemos la Hipótesis Generalizada del Continuo, la situación se vuelve más complicada.

Teorema 10.40 (Fórmula de Hausdorff) *Para cualesquiera ordinales α y β,*

$$\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}.$$

Demostración:

Si $\beta \geq \alpha + 1$, entonces $\aleph_{\alpha+1}^{\aleph_\beta} = 2^{\aleph_\beta}$, $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$, y $\aleph_{\alpha+1} \leq \aleph_\beta < 2^{\aleph_\beta}$; por lo tanto, la fórmula es válida. Así, supongamos que $\beta \leq \alpha$. Como $\aleph_\alpha^{\aleph_\beta} \leq \aleph_{\alpha+1}^{\aleph\beta}$ y $\aleph_{\alpha+1} \leq \aleph_{\alpha+1}^{\aleph_\beta}$, es suficiente mostrar que

$$\aleph_{\alpha+1}^{\aleph_\beta} \leq \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}.$$

Cada función $f : \omega_\beta \to \omega_{\alpha+1}$ es acotada, es decir, existe $\gamma < \omega_{\alpha+1}$ tal que $f(\xi) < \gamma$ para todo $\xi < \omega_\beta$ (puesto que $\omega_{\alpha+1}$ es regular y $\omega_\beta < \omega_{\alpha+1}$). Por lo tanto,

$$\omega_{\alpha+1}^{\omega_\beta} = \bigcup_{\gamma<\omega_{\alpha+1}} \gamma^{\omega_\beta}.$$

Ahora, cualquier $\gamma < \omega_{\alpha+1}$ tiene cardinalidad $|\gamma| \leq \aleph_\alpha$, y por el Ejercicio 10.2.6,

$$\left| \bigcup_{\nu<\omega_{\alpha+1}} \gamma^{\omega_\beta} \right| \leq \sum_{\gamma<\omega_{\alpha+1}} |\gamma|^{\aleph_\beta} \leq \sum_{\gamma<\omega_{\alpha+1}} \aleph_\alpha^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}. \quad \blacksquare$$

Teorema 10.41 (Fórmula Generalizada de Hausdorff) *Para cualquier número natural n y cualesquiera ordinales α y β,*

$$\aleph_{\alpha+n}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+n}.$$

Haciendo $\alpha = 0$ y usando el Lema 10.33, obtenemos el siguiente teorema.

Teorema 10.42 (Formula de Bernstein) *Para cualquier número natural n y cualquier número ordinal β,*

$$\aleph_n^{\aleph_\beta} = 2^{\aleph_\beta} \cdot \aleph_n.$$

Definición 10.43 Un cardinal infinito $\aleph_\alpha$ es *límite fuerte*, si $2^{\aleph_\beta} < \aleph_\alpha$ para todo $\beta < \alpha$.

Claramente un cardinal que es límite fuerte es un cardinal límite, ya que si $\aleph_\alpha = \aleph_{\gamma+1}$, entonces $2^{\aleph_\gamma} \geq \aleph_\alpha$. No cualquier cardinal límite es necesariamente límite fuerte: Si $2^{\aleph_0}$ fuera mayor que $\aleph_\omega$, entonces $\aleph_\omega$ sería un ejemplo. Sin embargo, *si suponemos la Hipótesis Generalizada del Continuo, entonces todo cardinal límite es un cardinal límite fuerte.*

Lema 10.44 *Si $\aleph_\alpha$ es un cardinal límite fuerte y si κ y λ son cardinales infinitos tales que $\kappa < \aleph_\alpha$ y $\lambda < \aleph_\alpha$, entonces $\kappa^\lambda < \aleph_\alpha$.*

DEMOSTRACIÓN:

$\kappa^\lambda \leq (\kappa \cdot \lambda)^{\kappa \cdot \lambda} = 2^{\kappa \cdot \lambda} < \aleph_\alpha$. ■

Sierpiński y Tarski introdujeron el siguiente tipo de cardinales.

Definición 10.45 Un número cardinal no numerable κ es *fuertemente inaccesible* si es regular y límite fuerte.

De acuerdo al comentario que precede al lema, todo cardinal fuertemente inaccesible es débilmente inaccesible, y si suponemos la Hipótesis Generalizada del Continuo, todo cardinal débilmente inaccesible es fuertemente inaccesible. La razón por la cual a tales cardinales se les llama inaccesibles es que ellos no pueden ser obtenidos por las operaciones conjuntistas usuales a partir de cardinales menores. Por ejemplo:

Si X tiene cardinalidad menor que κ, entonces $\mathcal{P}(X)$ tiene cardinalidad menor que κ.

Si cada $X \in \mathcal{S}$ tiene cardinalidad menor que κ, entonces $\bigcup \mathcal{S}$ tiene cardinalidad menor que κ.

Si $|X| < \kappa$ y $f : X \to \kappa$ es una función cualquiera, entonces $\sup f(X) < \kappa$.

Por lo anterior, no deber sorprender mucho que la existencia de cardinales inaccesibles sea independiente de los Axiomas **ZFC.**

Ejercicios 10.5

1. Pruebe el Lema 10.36.
2. Demuestre que si $2^{\aleph_\beta} \geq \aleph_\alpha$, entonces $\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$.
3. Demuestre que si existe $\gamma < \alpha$ tal que $\aleph_\gamma^{\aleph_\beta} \geq \aleph_\alpha$, digamos $\aleph_\gamma^{\aleph_\beta} = \aleph_\delta$, entonces $\aleph_\alpha^{\aleph_\beta} = \aleph_\delta$.

4. Sea α un ordinal límite y sea $\aleph_\beta$ tal que $cf(\aleph_\beta) < \aleph_\alpha$. Demuestre que si $\aleph_\xi^{\aleph_\beta} \leq \aleph_\alpha$ para todo $\xi < \alpha$, entonces $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$. (Sugerencia: si $X \subseteq \omega_\alpha$ es tal que $|X| = \aleph_\beta$, entonces $X \subseteq \omega_\xi$ para algún $\xi < \alpha$.)

5. Pruebe las Ecuaciones (10.5.1) y (10.5.2).

6. Demuestre el Teorema 10.39

7. Demuestre la Fórmula Generalizada de Hausdorff. (Sugerencia: use inducción sobre n.)

8. Demuestre la Fórmula de Bernstein.

9. Pruebe que:

   (a) $\aleph_1^{\aleph_0} = 2^{\aleph_0} \cdot \aleph_1$.
   (b) $\aleph_0^{\aleph_1} = 2^{\aleph_1}$.

10. Demuestre que la Hipótesis Generalizada del Continuo es equivalente a

$$\aleph_{\alpha+1}^{\aleph_\alpha} < \aleph_{\alpha+2}^{\aleph_\alpha}.$$

    para cualquier número ordinal α.

11. Si $\aleph_\alpha$ es fuertemente inaccesible y $\beta < \alpha$, entonces $\aleph_\alpha^{\aleph_\beta} = \aleph_\alpha$. (Sugerencia: aplique el Ejercicio 4.)

12. Demuestre que $\prod_{n<\omega} \aleph_n = \aleph_\omega^{\aleph_0}$. (Sugerencia: sean A_i $(i < \omega)$ subconjuntos infinitos mutuamente ajenos de ω. Entonces

$$\prod_{n<\omega} \aleph_n \geq \prod_{i<\omega} \left(\prod_{n\in A_i} \aleph_n \right) \geq \prod_{i<\omega} \left(\sum_{n\in A_i} \aleph_n \right) \geq \prod_{i<\omega} \aleph_\omega = \aleph_\omega^{\aleph_0}.$$

    La demostración de la otra desigualdad es más sencilla.)

13. Demuestre que $\aleph_\omega^{\aleph_1} = \aleph_\omega^{\aleph_0} \cdot 2^{\aleph_1}$. (Sugerencia:

$$\begin{aligned} \aleph_\omega^{\aleph_1} &= \left(\textstyle\sum_{n<\omega} \aleph_n\right)^{\aleph_1} \leq \left(\textstyle\prod_{n<\omega} \aleph_n\right)^{\aleph_1} \\ &= \textstyle\prod_{n<\omega} \aleph_n^{\aleph_1} = \prod_{n<\omega} (\aleph_n \cdot 2^{\aleph_1}) = \\ &= \left(\textstyle\prod_{n<\omega} \aleph_n\right) \cdot \left(2^{\aleph_1}\right)^{\aleph_0} = \aleph_\omega^{\aleph_0} \cdot 2^{\aleph_1}.) \end{aligned}$$

10.6 Medidas y Cardinales

[1]El concepto de medida es uno de los más importantes en el Análisis Abstracto, es fundamental para el desarrollo de la moderna teoría de integración. De particular importancia es la *medida de Lebesgue* de conjuntos de números reales. En el Ejemplo 8.18 se estableció que no cualquier conjunto de números reales es medible. La medida de Lebesgue es sin duda muy especial ya que coincide con la longitud de los intervalos y es invariante bajo traslaciones. Una clase de medida no tan restrictiva es la siguiente.

Definición 10.46 Sea X un conjunto no vacío. Una *medida σ-aditiva* sobre X es una función $\mu : \mathcal{P}(X) \to [0,1]$ tal que:

(a) $\mu(\emptyset) = 0, \quad \mu(X) = 1$,

(b) si $A \subseteq B$, entonces $\mu(A) \leq \mu(B)$,

(c) $\mu(\{x\}) = 0$ para cualquier $x \in X$,

(d) si $\{A_n\}_{n=0}^{\infty}$ es una familia de subconjuntos de X ajenos por pares, entonces

$$\mu\left(\bigcup_{n=0}^{\infty} A_n\right) = \sum_{n=0}^{\infty} \mu(A_n).$$

Como consecuencia de *(c)* y *(d)* de la definición, cualquier subconjunto a lo más numerable de X tiene medida 0. Por lo tanto, si hay una medida sobre X, entonces X es no numerable. Es claro que la existencia de medidas sobre X depende únicamente de la cardinalidad de X: Si X tiene una medida y $|X| = |X'|$ entonces X' también tiene una medida. Ya sabemos que la medida de Lebesgue no puede extenderse a $\mathcal{P}(\mathbf{R})$; pero la pregunta es: ¿Existe una medida σ-aditiva sobre $\mathbf{R}$? o equivalentemente ¿Existe una medida σ-aditiva sobre $2^{\aleph_0}$?

Mostraremos que este cuestionamiento muy natural del Análisis Abstracto está relacionada con el problema del continuo y sorpresivamente también con la materia de los cardinales inaccesibles. Este problema es el punto de partida para la investigación de los *cardinales grandes*, una teoría que exploraremos en las siguientes secciones.

El siguiente teorema fue formulado por Banach y Kuratowski en 1929.

Teorema 10.47 *Si existe una medida σ-aditiva sobre $2^{\aleph_0}$, entonces la Hipótesis del Continuo es falsa.*

---

[1]Esta sección y la siguiente requieren del material sobre ideales y filtros para el caso especial del álgebra Booleana $\mathcal{P}(X)$ expuestos en la Sección 8.5.

DEMOSTRACIÓN:

Supongamos que $2^{\aleph_0} = \aleph_1$ y que existe una medida σ-aditiva sobre el conjunto ω_1. En el álgebra de conjuntos $\mathcal{P}(\omega_1)$, consideremos el ideal de todos los subconjuntos de ω_1 con medida 0:

$$\mathcal{I} = \{X \subseteq \omega_1 : \mu(X) = 0\}.$$

Este ideal tiene las siguientes propiedades:

10.47(a) Para cualquier $\alpha \in \omega_1$, $\{\alpha\} \in \mathcal{I}$.

10.47(b) Si $X_n \in \mathcal{I}$ para todo $n \in \mathbf{N}$, entonces $\bigcup_{n=0}^{\infty} X_n \in \mathcal{I}$.

10.47(c) No existe $\mathcal{J}$, una familia no numerable de subconjuntos mutuamente ajenos de ω_1, tal que $X \notin \mathcal{I}$ para cualquier $X \in \mathcal{J}$.

Las dos primeras se obtienen de la definición de medida σ-aditiva. Para 10.47(c) supóngase que $\mathcal{J}$ es una de tales familias de conjuntos mutuamente ajenos. Para cada $n \in \mathbf{N} \setminus \{0\}$, sea

$$\mathcal{J}_n = \left\{X \in \mathcal{J} : \mu(X) \geq \tfrac{1}{n}\right\}.$$

Ya que $\mu(\omega_1) = 1$, cada $\mathcal{J}_n$ debe ser finita; además, como $\mathcal{J} = \bigcup_{n=1}^{\infty} \mathcal{J}_n$, se sigue que $\mathcal{J}$ es a lo más numerable.

Ahora construiremos una "matriz" $(A_{\alpha n})_{\alpha \in \omega_1,\, n \in \omega}$ de subconjuntos de ω_1 como sigue: Para cada $\xi < \omega_1$, existe una función $f_\xi{:}\omega \to \omega_1$ tal que $\xi \subseteq ran\, f_\xi$. Seleccionemos una de tales f_ξ para cada ξ, y sea

$$A_{\alpha n} = \{\xi < \omega_1 : f_\xi(n) = \alpha\} \qquad (\alpha < \omega_1,\, n < \omega).$$

La matriz $(A_{\alpha n})_{\alpha \in \omega_1,\, n \in \omega}$ tiene las siguientes propiedades:

10.47(d) Para cada n, si $\alpha \neq \beta$, entonces $A_{\alpha n} \cap A_{\beta n} = \emptyset$.

10.47(e) Para cualquier α, $\omega_1 \setminus \bigcup_{n=0}^{\infty} A_{\alpha n}$ es a lo más numerable.

En efecto, $\xi \in A_{\alpha n} \cap A_{\beta n}$ significa que $f_\xi(n) = \alpha$ y $f_\xi(n) = \beta$, luego $\alpha = \beta$. Por otra parte, el conjunto en 10.47(e) es a lo más numerable puesto que está incluido en el conjunto a lo más numerable α: Si $\xi \notin A_{\alpha n}$ para cualquier n, entonces $\alpha \notin ran\, f_\xi$ y así $\xi < \alpha$.

Sea $\alpha < \omega_1$ fijo. El conjunto ω_1 es unión de los conjuntos $A_{\alpha n}$ y de un conjunto a lo más numerable. Si $A_{\alpha n} \in \mathcal{I}$ para cada n, entonces $\omega_1 \in \mathcal{I}$ por

10.47(e), 10.47(a) y 10.47(b). Pero $\mu(\omega_1) = 1$, por lo cual ω_1 no pertenece a $\mathcal{I}$. Así, para cada $\alpha < \omega_1$ existe algún $n_\alpha \in \mathbf{N}$ tal que $A_{\alpha n_\alpha} \notin \mathcal{I}$. Puesto que ω_1 es no numerable y ω sí lo es, debe existir algún m tal que el conjunto $\{\alpha : n_\alpha = m\}$ es no numerable. Sea

$$\mathcal{J} = \{A_{\alpha m} : n_\alpha = m\}.$$

Esta es una familia no numerable de subconjuntos de ω_1. Por 10.47(d), los elementos de $\mathcal{J}$ son mutuamente ajenos, y $A_{\alpha m} \notin \mathcal{I}$ para cada $A_{\alpha m} \in \mathcal{J}$. Esto contradice 10.47(c).

La contradicción encontrada nos muestra que la suposición de que $2^{\aleph_0} = \aleph_1$ debe ser falsa, lo cual demuestra el teorema. ■

La demostración del teorema anterior puede modificarse para obtener un resultado más trascendente, a saber, la existencia de una medida σ-aditiva en un conjunto X, implica que X debe tener un cardinal gigantesco. Para llegar a establecer dicho resultado, necesitaremos de algunos resultados preliminares.

Primero supongamos que para algún conjunto X hay una medida σ-aditiva $\mu : \mathcal{P}(X) \to [0, 1]$. La demostración del Teorema 10.47 nos proporcionó un ideal $\mathcal{I}$ sobre X que satisface 10.47(a), 10.47(b) y 10.47(c).

Suposición 10.48 Sea κ el mínimo cardinal tal que para algún conjunto X con $|X| = \kappa$ existe un ideal sobre X con las propiedades 10.47(a), 10.47(b) y 10.47(c).

Suposición 10.49 Sea $\mathcal{I}$ un ideal sobre $X = \kappa$ con las propiedades 10.47(a), 10.47(b) y 10.47(c).

Lema 10.50 *Para cualquier $\lambda < \kappa$, si $\{A_\eta\}_{\eta<\lambda}$ es tal que $A_\eta \in \mathcal{I}$ para todo $\eta < \lambda$, entonces $\bigcup_{\eta<\lambda} A_\eta \in \mathcal{I}$.*

Demostración:

Si el lema es falso, existen $\lambda < \kappa$ y $\{A_\eta\}_{\eta<\lambda}$ tales que $A_\eta \in \mathcal{I}$, pero $\bigcup_{\eta<\lambda} A_\eta \notin \mathcal{I}$. Suponiendo que λ es el mínimo ordinal con tal propiedad, también podemos suponer que los conjuntos A_η son ajenos por pares, puesto que podemos reemplazar cada A_η por $A'_\eta = A_\eta \setminus \bigcup\{A_\nu : \nu < \eta\}$. Observe que

$$\bigcup_{\eta<\lambda} A'_\eta = \bigcup_{\eta<\lambda} A_\eta.$$

Sea

$$\mathcal{J} = \left\{ B \subseteq \lambda : \bigcup_{\eta\in B} A_\eta \in \mathcal{I} \right\}.$$

En el Ejercicio 10.6.1 se pide demostrar que $\mathcal{J}$ es un ideal sobre λ. Para cada $\eta \in \lambda$, $\{\eta\} \in \mathcal{J}$ ya que $A_\eta \in \mathcal{I}$; así, $\mathcal{J}$ satisface 10.47(a). Ahora, si $X_n \in \mathcal{J}$ para todo $n \in \omega$, entonces

$$\bigcup_{\eta \in X_n} A_\eta \in \mathcal{I}$$

para todo $n \in \omega$, y como $\mathcal{I}$ satisface 10.47(b) se tiene que

$$\bigcup_{n=0}^{\infty} \bigcup_{\eta \in X_n} A_\eta \in \mathcal{I}.$$

Pero esto significa que $\bigcup_{n=0}^{\infty} X_n \in \mathcal{J}$ puesto que

$$\bigcup_{n=0}^{\infty} \bigcup_{\eta \in X_n} A_\eta = \bigcup \left\{ A_\eta : \eta \in \bigcup_{n=0}^{\infty} X_n \right\}.$$

Así, $\mathcal{J}$ satisface 10.47(b). Finalmente, sea $\mathcal{K}$ una familia no numerable de subconjuntos mutuamente ajenos de λ tal que $X \notin \mathcal{J}$ para cualquier $X \in \mathcal{K}$. Si $X \in \mathcal{K}$, entonces

$$B_X = \bigcup \{A_\eta : \eta \in X\} \notin \mathcal{I}.$$

Dado que $\{A_\eta\}_{\eta<\lambda}$ y $\mathcal{K}$ son familias ajenas por pares, $\mathcal{K}' = \{B_X : X \in \mathcal{K}\}$ es una familia no numerable de subconjuntos mutuamente ajenos de κ tal que $Y \notin \mathcal{I}$ para cualquier $Y \in \mathcal{K}'$. Esto contradice que $\mathcal{I}$ satisface 10.47(c). Por lo tanto, $\mathcal{K}$ es a lo mas numerable. Así, $\mathcal{J}$ satisface 10.47(c). Por todo lo anterior, $\mathcal{J}$ es un ideal sobre $\lambda < \kappa$ con las propiedades 10.47(a), 10.47(b) y 10.47(c), contradiciendo la Suposición 10.48. ■

Corolario 10.51 *Si $Y \subseteq \kappa$, y $|Y| < \kappa$, entonces $Y \in \mathcal{I}$.*

Corolario 10.52 *κ es un cardinal regular no numerable.*

Demostración:

κ es no numerable dado que cualquier subconjunto a lo más numerable pertenece a $\mathcal{I}$. κ es regular, puesto que de otro modo κ sería la unión de menos que κ subconjuntos de cardinalidad menor que κ, y por lo tanto, pertenecería al ideal, una contradicción. ■

Teorema 10.53 *κ es débilmente inaccesible.*

DEMOSTRACIÓN:

En vista del Corolario 10.52 es suficiente demostrar que κ es un cardinal límite. Supongamos que $\kappa = \aleph_{\nu+1}$.

Para cada $\xi < \kappa$ podemos elegir una función $f_\xi : \omega_\nu \to \omega_{\nu+1}$ tal que $\xi \subseteq ran\, f_\xi$. Para $\alpha < \omega_{\nu+1}$ y $\eta < \omega_\nu$ sea

$$A_{\alpha\eta} = \{\xi < \kappa : f_\xi(\eta) = \alpha\}.$$

Como en la demostración del Teorema 10.47, se puede mostrar que la matriz $(A_{\alpha\eta})_{\alpha,\eta}$ tiene las siguientes propiedades:

10.53(a) Para cualquier η, si $\alpha \neq \beta$, entonces $A_{\alpha\eta} \cap A_{\beta\eta} = \emptyset$.

10.53(b) Para cualquier α, $\left|\kappa \setminus \bigcup_{\eta<\omega_\nu} A_{\alpha\nu}\right| \leq \aleph_\nu$.

Siguiendo la demostración del Teorema 10.47, pero usando el Lema 10.50 en lugar de 10.47(b), se muestra que para cada $\alpha < \omega_{\nu+1}$ existe algún $\eta < \omega_\nu$ tal que $A_{\alpha\eta} \notin \mathcal{I}$. Y el mismo argumento que antes demuestra la existencia de una familia $\mathcal{J}$, de cardinalidad $\aleph_{\nu+1}$ (por lo tanto, no numerable), de conjuntos ajenos por pares que no pertenecen a $\mathcal{I}$. Esto contradice la propiedad 10.47(c), y por lo tanto, κ no puede ser un cardinal sucesor. ■

Finalmente tenemos el resultado que resume nuestro estudio.

Corolario 10.54 *Si hay una medida σ-aditiva sobre un conjunto X, entonces existe algún cardinal débilmente inaccesible $\kappa \leq |X|$.*

Corolario 10.55 *Si existe una medida σ-aditiva sobre $2^{\aleph_0}$, entonces $2^{\aleph_0} \geq \kappa$ para algún cardinal débilmente inaccesible κ.*

Ejercicios 10.6

1. Pruebe que la familia

$$\mathcal{J} = \left\{ B \subseteq \lambda : \bigcup_{\eta\in B} A_\eta \in \mathcal{I} \right\},$$

que apareció en la demostración del Lema 10.50 es un ideal sobre λ.

10.7 Cardinales Medibles

En la sección anterior demostramos que la existencia de medidas σ-aditivas implica la existencia de cardinales débilmente inaccesibles. Este resultado es solamente un ejemplo de la vasta cantidad de resultados que constituyen la teoría de los llamados cardinales grandes. En esta sección estudiaremos el prototipo más conocido de cardinales grandes, los cardinales medibles; cuyo origen proviene de los trabajos de Banach, Kuratowski, Tarski y Ulam alrededor de 1930.

Definición 10.56 Sea X un conjunto y sea μ una medida σ-aditiva sobre X. Decimos que μ es una *medida* 2*-valuada* si $\mu(A)$ es 0 o 1 para cualquier $A \subseteq X$ y satisface en (a) a (d) de la Definición 10.46.

Lema 10.57 *Si μ es una medida* 2*-valuada sobre X, entonces*

$$\mathcal{U} = \{A \subseteq X : \mu(A) = 1\}$$

es un ultrafiltro no principal sobre X, y si $\{A_n\}_{n=0}^{\infty}$ es tal que $A_n \in \mathcal{U}$ para cada $n \in \mathbf{N}$, entonces $\bigcap_{n=0}^{\infty} A_n \in \mathcal{U}$.

Demostración:

La verificación de que $\mathcal{U}$ es un ultrafiltro es fácil, y la dejamos para el lector. $\mathcal{U}$ no es principal, dado que μ no es trivial. $\mathcal{U}$ satisface la segunda parte del lema porque μ es σ-aditiva. ■

La propiedad de la segunda parte del Lema 10.57 se llama σ*-completitud.* El recíproco de la primera parte del Lema 10.57 también es cierto: si $\mathcal{U}$ es un ultrafiltro σ-completo no principal, entonces la función $\mu : \mathcal{P}(X) \to \{0, 1\}$ definida por

$$\mu(A) = \begin{cases} 1 & \text{si } A \in \mathcal{U}, \\ 0 & \text{si } A \notin \mathcal{U}. \end{cases}$$

es una medida 2-valuada sobre X.

Así, el problema de la existencia de una medida 2-valuada es equivalente al problema de la existencia de ultrafiltros σ-completos no principales. Investigaremos ahora este problema. Primero generalizaremos la definición de σ-completitud.

Definición 10.58 Sea κ un cardinal no numerable.

(a)Un filtro $\mathcal{F}$ sobre X es κ*-completo* si para cualquier cardinal $\lambda < \kappa$, si $A_\alpha \in \mathcal{F}$ para toda $\alpha < \lambda$, entonces $\bigcap_{\alpha<\lambda} A_\alpha \in \mathcal{F}$.

(b) Un ideal $\mathcal{I}$ sobre X es *κ-completo* si para cualquier cardinal $\lambda < \kappa$, si $A_\alpha \in \mathcal{I}$ para toda $\alpha < \lambda$, entonces $\bigcup_{\alpha<\lambda} A_\alpha \in \mathcal{I}$.

La $\aleph_1$-completitud es de hecho la σ-completitud. Ahora formularemos un lema que está estrechamente relacionado con el Lema 10.50

Lema 10.59 *Si existe un ultrafiltro σ-completo no principal entonces existe un cardinal no numerable κ y un ultrafiltro κ-completo no principal.*

Demostración:

Sea κ el mínimo cardinal κ tal que existe un ultrafiltro σ-completo no principal sobre κ, y sea $\mathcal{U}$ uno de tales ultrafiltros. Demostraremos que $\mathcal{U}$ es κ-completo (note que al ser $\mathcal{U}$ σ-completo, se deduce que κ es no numerable).

Sea $\mathcal{I}$ el ideal dual a $\mathcal{U}$; o sea, $\mathcal{I} = \mathcal{P}(X) \setminus \mathcal{U}$. $\mathcal{I}$ es un ideal primo σ-completo sobre κ; probaremos que $\mathcal{I}$ es κ-completo. Si no lo fuera, entonces existen $\lambda < \kappa$ y $\{A_\eta\}_{\eta<\lambda}$ tales que $A_\eta \in \mathcal{I}$ para cada $\eta < \lambda$ pero $\bigcup_{\eta<\lambda} A_\eta \notin \mathcal{I}$. Como en el Lema 10.50, podemos suponer que los A_η son mutuamente ajenos. Sea

$$\mathcal{J} = \left\{ B \subseteq \lambda : \bigcup_{\eta\in B} A_\eta \in \mathcal{I} \right\}.$$

$\mathcal{J}$ es un ideal σ-completo no principal; no es principal dado que $X_\eta \in \mathcal{J}$ para cada $\eta \in \lambda$. Así, el dual $\mathcal{P}(X) \setminus \mathcal{J}$ de $\mathcal{J}$ es un ultrafiltro σ-completo no principal sobre λ.

Pero $\lambda < \kappa$; esto contradice la suposición de que κ es el mínimo cardinal sobre el cual existe un ultrafiltro σ-completo no principal. Así, $\mathcal{U}$ es κ-completo. ■

Definición 10.60 Un *cardinal medible* es un cardinal no numerable κ sobre el cual existe un ultrafiltro κ-completo no principal.

La discusión planteada antes de la Definición 10.58 muestra que los cardinales medibles están relacionados con el problema de la medida investigado en la sección anterior. La existencia de un cardinal medible es equivalente a la existencia de una medida 2-valuada. Ulam y Tarski descubrieron que los cardinales medibles deben ser fuertemente inaccesibles.

Teorema 10.61 *Cualquier cardinal medible es fuertemente inaccesible.*

Demostración:

Sea κ un cardinal medible, y sea $\mathcal{U}$ un ultrafiltro κ-completo no principal sobre κ.

Sea $\mathcal{I}$ el ideal dual de $\mathcal{U}$; $\mathcal{I}$ es un ideal primo. Cualquier conjunto singular pertenece a $\mathcal{I}$, y por la κ-completitud, cualquier $A \subset \kappa$ de cardinalidad menor que κ pertenece a $\mathcal{I}$. Si κ fuera singular, el conjunto κ también pertenecería a $\mathcal{I}$, por κ-completitud; contradiciendo que $\mathcal{I}$ es un ideal propio (compare con el Corolario 10.52). Por lo tanto, κ es regular.

Ahora supongamos que κ no es límite fuerte. Entonces existe $\lambda < \kappa$ tal que $2^\lambda \geq \kappa$. Así, hay un conjunto $X \subseteq \{0,1\}^\lambda$ de cardinalidad κ sobre el cual hay también un ultrafiltro κ-completo no principal, digamos $\mathcal{V}$. Para cada $\alpha < \lambda$, exactamente uno de los conjuntos

$$\{f \in X : f(\alpha) = 0\} \qquad \text{y} \qquad \{f \in X : f(\alpha) = 1\} \tag{10.7.1}$$

pertenece a $\mathcal{V}$; llamemos A_α a ese conjunto. Así, para cada $\alpha < \lambda$ tenemos que $A_\alpha \in \mathcal{V}$, y por κ-completitud, $X = \bigcap_{\alpha<\lambda} A_\alpha$ también es miembro de $\mathcal{V}$. Pero hay a lo más una función $f \in X$ que pertenece a todo A_α: el valor de f en α está determinado por la elección de uno de los conjuntos en (10.7.1). Por lo tanto, $|X| \leq 1$; lo cual es una contradicción. Por lo que κ es límite fuerte y por lo tanto, κ es fuertemente inaccesible. ■

10.8 Otros Cardinales Grandes

Definición 10.62 Sea κ un cardinal infinito. Un *árbol de altura* κ es un conjunto T de sucesiones transfinitas con las siguientes propiedades:

(a) $dom\, s < \kappa$ para cualquier $s \in T$,

(b) si $s \subseteq t$ y $t \in T$, entonces $s \in T$,

(c) para cualquier $\eta < \kappa$ existe $s \in T$ con $dom\, s = \eta$.

A los elementos de un árbol se les suele llamar *nodos*. Un *sucesor de un nodo* $s \in T$ es una $t \in T$ tal que $t \supseteq s$ y $dom\, t = (dom\, s) + 1$. Una *rama en* T es una sucesión transfinita b con la propiedad de que todos los segmentos iniciales propios de b están en T pero $b \notin T$.

Teorema 10.63 *Sea κ un cardinal medible. Si T es un árbol de altura κ tal que cada nodo tiene menos que κ sucesores, entonces T tiene una rama de longitud κ.*

DEMOSTRACIÓN:

Para cada $\alpha < \kappa$, sea T_α el conjunto de todas las $s \in T$ de longitud α. Como κ es un cardinal fuertemente inaccesible, se sigue, por inducción sobre α, que $|T_\alpha| < \kappa$ para todo $\alpha < \kappa$. Por lo tanto, $|T| \leq \kappa$. Por la Definición 10.62(c), $|T| = \kappa$. Sea $\mathcal{U}$ un ultrafiltro κ-completo no principal sobre T.

Encontraremos una rama de longitud κ como sigue. Por inducción sobre α mostraremos que para cada α existe un único $s_\alpha \in T$ tal que

$$\{t \in T : s_\alpha \subseteq t\} \in \mathcal{U} \tag{10.8.1}$$

y que $s_\alpha \subset s_\beta$ cuando $\alpha < \beta$. Primero, $s_0 = \emptyset$. Dada s_α, y suponiendo (10.8.1), notamos que el conjunto $\{t \in T : s_\alpha \subseteq t\}$ es la unión de $\{s_\alpha\}$ y los conjuntos $\{t \in T : u \subseteq t\}$ donde u corre sobre todos los sucesores de s_α. Como $\mathcal{U}$ es un ultrafiltro κ-completo y s_α tiene menos que κ sucesores, existe un único sucesor $u = s_{\alpha+1}$ tal que

$$\{t \in T : s_{\alpha+1} \subseteq t\} \in \mathcal{U}.$$

Cuando η es un ordinal límite menor que κ y si $\{s_\alpha\}_{\alpha<\eta} \subseteq T$ cumple que $s_\alpha \subset s_\beta$ si $\alpha < \beta$, y todos los s_α satisfacen (10.8.1), entonces definimos $s_\eta = \bigcup_{\alpha<\eta} s_\alpha$. Tenemos que

$$\{t \in T : s_\eta \subseteq t\} = \bigcap_{\alpha<\eta} \{t \in T : s_\alpha \subseteq t\} \tag{10.8.2}$$

y puesto que $\mathcal{U}$ es κ-completo, el conjunto de (10.8.2) pertenece a $\mathcal{U}$. Es claro que $b = \bigcup \{s_\alpha : \alpha < \kappa\}$ es una rama en T, de longitud κ. ■

Tarski introdujo el siguiente tipo de cardinales.

Definición 10.64 Un cardinal fuertemente inaccesible κ se llama *débilmente compacto* si para cualquier árbol de altura κ con menos de κ sucesores en cada nodo, existe una rama de T de longitud κ.

Los cardinales débilmente compactos son un grupo de cardinales grandes más débiles que los cardinales medibles, pero aún bastante poderosos. La razón del nombre "débilmente compacto" es que estos cardinales satisfacen un cierto teorema de compacidad en lógica.

Una pregunta natural después de definir a los cardinales débilmente compactos es: ¿Cuáles son los cardinales compactos? Los cardinales compactos pueden ser definidos de varias maneras diferentes, para nosotros, la más sencilla es la que se da en términos de una generalización del Teorema del Ultrafiltro.

Definición 10.65 Un cardinal regular no numerable κ es *compacto* (o *fuertemente compacto*) si para cualquier conjunto X, todo filtro (propio) κ-completo sobre X puede extenderse a un ultrafiltro κ-completo sobre X.

Obviamente, cualquier cardinal compacto es un cardinal medible, porque cualquier ultrafiltro sobre κ que extiende al filtro

$$\{A \subseteq \kappa : |\kappa \setminus A| < \kappa\},$$

es no principal.

Definición 10.66 Sea κ un cardinal regular no numerable. Decimos que un conjunto $C \subseteq \kappa$ es *cerrado y no acotado* en κ si:

(a) Para cualquier sucesión de longitud $\gamma < \kappa$,

$$\alpha_0 < \alpha_1 < \cdots < \alpha_\xi < \cdots \qquad (\xi < \gamma),$$

de elementos de C, se tiene que $\lim_{\xi\to\gamma} \alpha_\xi \in C$. ($C$ es cerrado.)

(b) Para cualquier $\alpha < \kappa$, existe un $\beta > \alpha$ tal que $\beta \in C$. (C es no acotado.)

Ejemplo 10.67 El conjunto de todos los ordinales límites $\alpha < \kappa$ es cerrado y no acotado en κ.

La demostración del siguiente lema es sencilla y preferimos dejarla para el lector.

Lema 10.68 *Si C y D son conjuntos cerrados y no acotados, entonces $C \cap D$ es cerrado no acotado.*

La familia de todos los subconjuntos cerrados y no acotados de κ tiene la propiedad de la intersección finita. El filtro generado por los conjuntos cerrados y no acotados consiste de todos los $X \subseteq \kappa$ que contienen un subconjunto cerrado y no acotado. Llamaremos a este filtro el *filtro cerrado y no acotado* sobre κ.

Definición 10.69 Sea $f : \kappa \to \kappa$ una función; decimos que

(a) f es *continua* si

$$f(\alpha) = \lim_{\xi\to\alpha} f(\xi)$$

para cualquier ordinal límite $\alpha < \kappa$ distinto de 0.

(b) f es *normal* si es creciente y continua.

El rango de una función normal es un conjunto cerrado y no acotado: las funciones $f_\alpha(\beta) = \alpha + \beta$, $g_\alpha(\beta) = \alpha \cdot \beta$ y $h_\alpha(\beta) = \alpha^\beta$ son normales (esto se sigue de la definición y su monotonía). Por lo tanto, existen muchos conjuntos cerrados y no acotados. El siguiente resultado nos dice que el filtro cerrado y no acotado sobre κ es κ-completo.

Proposición 10.70 *La intersección de menos que κ subconjuntos cerrados y no acotados es un conjunto cerrado y no acotado.*

Demostración:

Probaremos, por inducción sobre $\gamma < \kappa$, que la intersección de una familia $\{C_\alpha\}_{\alpha<\gamma}$ de subconjuntos cerrados no acotados de κ es cerrada y no acotada. El paso de inducción para ordinales sucesores lo establece el Lema 10.68. Si γ es un ordinal límite, suponemos que el lema es válido para cualquier $\alpha < \gamma$. Entonces podemos reemplazar cada C_α por $\bigcap_{\xi<\alpha} C_\xi$ y obtener una sucesión decreciente con la misma intersección. Así, supongamos que

$$C_0 \supseteq C_1 \supseteq \cdots \supseteq \cdots C_\alpha \supseteq \cdots \quad (\alpha < \xi)$$

son cerrados no acotados, y sea $C = \bigcap_{\alpha<\gamma} C_\alpha$.

Es fácil ver que C es cerrado. Para mostrar que C es no acotado, sea $\alpha < \kappa$. Construiremos una sucesión

$$\beta_0 < \beta_1 < \cdots < \beta_\xi < \cdots \qquad (\xi < \gamma)$$

como sigue: Sea $\beta_0 \in C_0$ tal que $\beta_0 > \alpha$, y para cada $\xi < \gamma$, sea $\beta_\xi \in C_\xi$ tal que

$$\beta_\xi > \sup\{\beta_\nu : \nu < \xi\}.$$

Como κ es regular y $\gamma < \kappa$, tal sucesión existe y su límite β es menor que κ. Para cada $\eta < \gamma$, β es el límite de una sucesión $(\beta_\xi)_{\eta<\xi<\gamma}$ en C_η, y así $\beta \in C_\eta$. Por lo tanto, $\beta \in C$. ■

Definición 10.71 Sea κ un cardinal regular no numerable. Decimos que un conjunto $S \subseteq \kappa$ es *estacionario en* κ si $S \cap C \neq \emptyset$ para cualquier subconjunto cerrado y no acotado de κ. Un conjunto que no es estacionario se llamará *delgado.*

Note que la familia de todos los conjuntos delgados es el ideal dual del filtro cerrado y no acotado.

Sea κ un cardinal fuertemente inaccesible. El conjunto de todos los cardinales menores que κ es un subconjunto cerrado y no acotado de κ, y así es

también el conjuntos de todos los cardinales límite fuerte. En efecto, el conjunto de todos los cardinales límite fuerte menores que κ es cerrado; para mostrar que es no acotado, si $\lambda < \kappa$, un cardinal límite fuerte mayor que λ puede obtenerse mediante el límite de $\lambda,\ 2^{\lambda},\ 2^{2^{\lambda}}, \ldots$.

Si κ es el mínimo cardinal inaccesible (suponiendo su existencia), entonces todos los cardinales límites fuerte menores que κ son singulares, y así, el conjunto de todos los cardinales límite fuerte y singulares menores que κ es cerrado y no acotado. Si κ es el α-ésimo cardinal fuertemente inaccesible, donde $\alpha < \kappa$, entonces el conjunto de todos los cardinales regulares menores que κ sigue siendo delgado. En otras palabras, los cardinales regulares menores que κ forman un conjunto delgado en κ.

Definición 10.72 Un cardinal fuertemente inaccesible κ se llama *cardinal de Mahlo* si el conjunto de todos los cardinales regulares menores que κ es estacionario en κ.

De la discusión anterior a la definición, se deduce que para un cardinal de Mahlo κ, el conjunto de todos los cardinales fuertemente inaccesibles menores que κ es estacionario, y κ es el κ-ésimo cardinal inaccesible.

Definición 10.73 Un *cardinal débilmente de Mahlo*, es un cardinal κ que es inaccesible y el conjunto de todos los cardinales regulares menores que κ es estacionario.

Puede demostrarse que cualquier cardinal débilmente compacto es un cardinal de Mahlo, desgraciadamente la demostración está lejos de nuestro alcance. P. Mahlo se considera el autor de los cardinales débilmente de Mahlo. Él no trabajó con cardinales fuertemente inaccesibles.

Sean $\alpha,\ \kappa,\ \lambda$ cardinales y $n < \omega$. La notación de *flecha*

$$\alpha \to (\kappa)^n_{\lambda}$$

denota la siguiente relación de partición: si $\{P_\eta\}_{\eta<\lambda}$ es una partición de

$$[\alpha]^n = \{X \subseteq \alpha : |X| = n\},$$

entonces existen $A \subseteq \alpha$ y $\eta < \lambda$ tales que

$$|A| = \kappa, \quad \text{y} \quad [A]^n \subseteq P_\eta.$$

Equivalentemente, $\alpha \to (\kappa)^n_{\lambda}$ si para toda función $f : [\alpha]^n \to \lambda$, existe $A \in [\alpha]^{\kappa}$ tal que f restingida a $[A]^n$ es constante. El conjunto A se llama *homogéneo* para la familia $\{P_\eta\}_{\eta<\lambda}$.

El siguiente hecho es obvio: si $\alpha' \geq \alpha,\ \kappa \leq \kappa',\ \lambda' \leq \lambda$, y $\alpha \to (\kappa)^n_\lambda$ entonces $\alpha' \to (\kappa')^n_{\lambda'}$.

Definición 10.74 Un cardinal infinito κ es un *cardinal de Ramsey* si

$$\kappa \to (\kappa)^2_2.$$

Definición 10.75 Un cardinal infinito κ es un *cardinal de Hausdorff* si para cualquier orden lineal $\preceq$ sobre κ existe un subconjunto de κ de cardinalidad κ el cual es, o bien ordenado por $\preceq$ o bien ordenado por el orden dual $\preceq^{-1}$.

Teorema 10.76 *Cualquier cardinal de Ramsey es un cardinal de Hausdorff.*

Demostración:

Sea κ un cardinal de Ramsey y sea $\preceq$ un orden lineal sobre κ. Pongamos P_0 como el conjunto de todos los pares no ordenados $\{\xi, \zeta\}$ tales que o bien $\xi < \zeta < \kappa$ y $\xi \preceq \zeta$ o $\zeta < \xi < \kappa$ y $\zeta \preceq \xi$, y P_1 como el conjunto de todos los $\{\xi, \zeta\}$ tales que o bien $\xi < \zeta < \kappa$ y $\zeta \preceq \xi$ o $\zeta < \xi < \kappa$ y $\xi < \zeta$. Así, P_0 es el conjunto de pares no ordenados de distintos elementos de κ en los cuales el buen orden de κ coincide con el orden lineal $\preceq$ y P_1 es el conjunto de pares ordenados en los cuales los dos ordenes difieren. Tenemos que

$$[\kappa]^2 = P_0 \cup P_1,$$

y como κ es un cardinal de Ramsey, existe $A \subseteq \kappa$ tal que o bien $[A]^2 \subseteq P_0$ o $[A]^2 \subseteq P_1$. Si $[A]^2 \subseteq P_0$ entonces A está bien ordenado por $\preceq$, y si $[A]^2 \subseteq P_1$ entonces A está bien ordenado por $\preceq^{-1}$. ■

Para demostrar el siguiente teorema, que nos revelará el tamaño de los cardinales de Hausdorff, necesitaremos de lo siguiente.

Sea α un ordinal. Si $a, b \in \{0,1\}^\alpha$ y $a \neq b$ consideremos

$$\xi(a,b) = \min\{\xi < \alpha : a_\xi \neq b_\xi\},$$

y hacemos $a \leq b$ si $a = b$ o $a \neq b$ y $a_{\xi(a,b)} < b_{\xi(a,b)}$. Como α es un conjunto bien ordenado, $\leq$ está bien definido y es un orden lineal sobre $\{0,1\}^\alpha$. Un elemento de $\{0,1\}^\alpha$ es una sucesión diádica de longitud α y $\leq$ es el orden lexicográfico sobre $\{0,1\}^\alpha$.

Lema 10.77 *Si A es un conjunto bien ordenado bajo el orden lexicográfico o bajo su dual en $\{0,1\}^{\omega_\alpha}$, entonces $|A| \leq \aleph_\alpha$.*

DEMOSTRACIÓN:

Demostraremos la proposición cuando A es considerado con el orden lexicográfico; las modificaciones de la demostración para el caso en que A es bien ordenado por el orden dual se dejan para el lector.

Supongamos sin pérdida de generalidad (omitiendo si es necesario una cantidad finita de elementos), que A no tiene elemento máximo y que $\aleph_\alpha < |A|$. Afirmamos que existe un ordinal $\xi < \omega_\alpha$ para el cual existen funciones $f, g : \omega_{\alpha+1} \to A$ tales que

(i) f y g son crecientes e inyectivas,
(ii) $f(\eta) < g(\eta) < f(\eta+1)$ y
(iii) $\xi(f(\eta), g(\eta)) = \xi$ para $\eta < \omega_{\alpha+1}$.

Sea $s : A \to A$ tal que $s(a)$ es el sucesor inmediato de a en A, y sea

$$A_\xi = \{a \in A : \xi(a, s(a)) = \xi\}$$

para cada $\xi < \omega_\alpha$. Como $A = \bigcup_{\xi<\omega_\alpha} A_\xi$, existe $\xi < \omega_\alpha$ tal que $|A_\xi| > \omega_\alpha$. Como A_ξ también es bien ordenado, existen un único ordinal β y un único isomorfismo de orden $h : \beta \to A_\xi$. Note que $\omega_{\alpha+1} \leq \beta$. Hagamos

$$f = h\,|_{\omega_{\alpha+1}} \qquad \text{y} \qquad g = s \circ f.$$

Es claro que f, g y ξ satisfacen las condiciones *(i)* y *(iii)*; y que

$$f(\eta) < s(f(\eta)) = g(\eta) \leq f(\eta+1)$$

para $\eta < \omega_{\alpha+1}$; además, como $f(\eta)_\xi = 0 < 1 = g(\eta)_\xi$ para $\eta < \omega_{\alpha+1}$, tenemos que $f(\eta+1) \neq g(\eta)$. La prueba de la afirmación está completa.

Ahora sea ξ el mínimo ordinal menor que ω_α para el cual existen las funciones f, g que satisfacen las condiciones *(i)*, *(ii)* y *(iii)*.

Sea

$$B_\zeta = \{g(\eta) : \eta < \omega_{\alpha+1} \text{ y } \xi(g(\eta),\, f(\eta+1)) = \zeta\}$$

para cada $\zeta < \xi$. Como $g(\eta)_\xi = 1$, $f(\eta+1)_\xi = 0$ y $g(\eta) < f(\eta+1)$, se sigue que $\xi(g(\eta),\, f(\eta+1)) < \xi$ para $\eta < \omega_{\alpha+1}$; por lo tanto,

$$g\left(\{\eta\}_{\eta<\omega_{\alpha+1}}\right) = \bigcup_{\zeta<\xi} B_\zeta.$$

Así, existe $\zeta < \xi$ tal que $|B_\zeta| = \aleph_{\alpha+1}$. Nuevamente, al ser B_ζ un conjunto bien ordenado, existe un ordinal $\beta' \geq \omega_{\alpha+1}$ y un isomorfismo de orden $h' : \beta' \to B_\zeta$. Sea

$$f' = h'\,|_{\omega_{\alpha+1}}$$

y definamos $g' : \omega_{\alpha+1} \to A$ mediante

$$g'(\eta) = f(g^{-1}(f'(\eta)) + 1).$$

Como $f'\left(\{\eta\}_{\eta<\omega_{\alpha+1}}\right) \subseteq g\left(\{\eta\}_{\eta<\omega_{\alpha+1}}\right)$, la función g' está bien definida. Es claro que f' y g' son funciones crecientes e inyectivas de $\omega_{\alpha+1}$ en A, $f'(\eta) < g'(\eta)$ para $\eta < \omega_{\alpha+1}$, y $\xi(f'(\eta), g'(\eta)) = \zeta$ para $\eta < \omega_{\alpha+1}$; por lo tanto,

$$g'(\eta) = f(g^{-1}(f'(\eta)) + 1) < g(g^{-1}(f'(\eta)) + 1) \leq f'(\eta + 1).$$

Pero como $f'(\eta+1)$ es el sucesor inmediato de $f'(\eta)$ en $ran\, f'$, $g(g^{-1}(f'(\eta))+1)$ es el sucesor inmediato de $f'(\eta)$ en $ran\, g$ y $ran\, f' \subseteq ran\, g$.

Se sigue que ζ, f' y g' satisfacen las condiciones *(i), (ii)* y *(iii)* con $\zeta < \xi$; contradiciendo la elección de ξ. ■

Teorema 10.78 *Cualquier cardinal de Hausdorff es fuertemente inaccesible.*

Demostración:

Sea κ un cardinal de Hausdorff. Veamos primero que κ es regular. Supóngase que $cf(\kappa) < \kappa$ y sea $\{A_\xi : \xi < \kappa\}$ una familia de subconjuntos de κ tales que:

$$\begin{gathered} |A_\xi| < \kappa \text{ para cada } \xi < cf(\kappa), \\ A_\xi \cap A_\zeta = \emptyset \text{ para } \xi < \zeta < cf(\kappa), \text{ y} \\ \kappa = \textstyle\bigcup_{\xi<cf(\kappa)} A_\xi. \end{gathered}$$

Definamos una relación $\preceq$ en κ por la siguiente regla: $\eta \prec \eta'$ si y sólo si o bien existen $\xi < \xi' < cf(\kappa)$ tales que $\eta \in A_\xi$ y $\eta' \in A_{\xi'}$ o existe $\xi < cf(\kappa)$ tal que $\eta, \eta' \in A_\xi$ y $\eta' < \eta$. Entonces $\preceq$ es un orden lineal sobre κ. Si A es un subconjunto de κ bien ordenado por $\preceq$ entonces, puesto que $\preceq^{-1}$ es un buen orden sobre A_ξ para cada $\xi < cf(\kappa)$, tenemos que $|A \cap A_\xi| < \aleph_0$ para $\xi < cf(\xi)$; y por lo tanto,

$$|A| = \sum_{\xi<cf(\kappa)} |A \cap A_\xi| \leq \aleph_0 \cdot cf(\kappa) < \kappa.$$

Si A es $\preceq^{-1}$-bien ordenado, entonces existe $\zeta < cf(\kappa)$ tal que el elemento máximo de A (en el orden $\preceq$) es un elemento de A_ζ. Entonces $A \subseteq \bigcup_{\xi<\zeta} A_\xi$; por lo tanto,

$$|A| \leq \sum_{\xi<\zeta} |A_\xi| < \kappa.$$

Así, κ no es un cardinal de Hausdorff; lo cual es una contradicción.

Ahora veamos que κ es límite fuerte. Sea λ un cardinal tal que $\kappa \leq 2^{\lambda}$. Entonces hay un subconjunto A de $\{0,1\}^{\lambda}$ tal que $|A| = \kappa$. Como A está linealmente ordenado (en el orden inducido por $\{0,1\}^{\lambda}$) y κ es un cardinal de Hausdorff, existe un subconjunto B de A tal que $|B| = \kappa$, y B es bien ordenado o es bien ordenado bajo el dual del orden lexicográfico. De acuerdo al lema anterior, B debe tener cardinalidad a lo más λ. Así, $\kappa = |B| \leq \lambda$. ■

Para terminar con esta sección presentamos un teorema que asegura la equivalencia de tres de los tipos de cardinales antes presentados, a pesar de estar definidos de manera completamente diferente. Desafortunadamente la demostración de dicho teorema requiere de un estudio más profundo de las propiedades de estos cardinales.

Teorema 10.79 *Para cualquier cardinal infinito κ las siguientes proposiciones son equivalentes:*

(a) κ es un cardinal débilmente compacto,

(b) κ es un cardinal de Ramsey,

(c) κ es un cardinal de Hausdorff.

Ejercicios 10.8

1. Demuestre el Lema 10.68.

2. (a) Muestre que el conjunto de puntos fijos (es decir, $f(\alpha) = \alpha$) de una función normal es cerrado y no acotado.

   (b) Si $f : \kappa \to \kappa$, entonces el conjunto de todos los $\alpha < \kappa$ tales que

   $$f(\{\xi : \xi < \alpha\}) \subseteq \alpha$$

   es cerrado y no acotado.

3. Demuestre que si $C_\alpha \subseteq \kappa$ es cerrado y no acotado para cada $\alpha \in \kappa$, entonces $\left\{\beta \in \kappa : \beta \in \bigcap_{\alpha \in \beta} C_\alpha\right\}$ es cerrado y no acotado en κ.

4. Demuestre que si $S \subseteq \kappa \setminus \{0\}$ es estacionario en κ y $f : S \to \kappa$ es una función tal que $f(\alpha) < \alpha$ para todo $\alpha \in S$, entonces existe un subconjunto estacionario $S' \subseteq S$ de modo que f restringida a S' es constante.

11

Dos Tópicos Especiales

11.1 El Problema de Souslin

Definición 11.1 Sea $(A, \leq)$ un conjunto linealmente ordenado.

(a) Se dice que $(A, \leq)$ es *denso s*i para cualesquiera $a, b \in A$ con $a < b$ existe $c \in A$ tal que $a < c < b$.

(b) Se dice que $(A, \leq)$ es *no acotado* si no tiene elementos máximo y mínimo.

Vamos a dar otro teorema de Cantor, el cual muestra que cualquier conjunto numerable linealmente ordenado que es denso y no acotado es isomorfo al conjunto de los números racionales $\mathbf{Q}$ con su orden usual.

Teorema 11.2 *Cualesquiera dos conjuntos linealmente ordenados, numerables, densos y no acotados son isomorfos.*

Demostración:

Sean $A = \{a_n : n \in \mathbf{N}\}$ y $B = \{b_n : n \in \mathbf{N}\}$ conjuntos que satisfacen las suposiciones del teorema. Para simplificar la notación, usaremos el mismo símbolo para denotar las relaciones de orden en ambos conjuntos.

Definiremos primero dos biyecciones $\phi, \psi : \mathbf{N} \to \mathbf{N}$ de tal manera que la función $f : A \to B$ dada por $f(a_{\phi(n)}) = b_{\psi(n)}$ constituya un isomorfismo de orden. Para este propósito, sea $\phi(0) = \psi(0) = 0$. Ahora sean

$$F_n = \big\{k \in \mathbf{N} : a_k \neq a_{\phi(j)},\ \ 0 \leq j \leq n\big\}$$

$$G_n = \big\{k \in \mathbf{N} : (b_{\psi(j)} < b_k) \Leftrightarrow (a_{\phi(j)} < a_{\phi(n+1)}),\ \ 0 \leq j \leq n\big\}$$

$$H_n = \big\{k \in \mathbf{N} : b_k \neq b_{\psi(j)},\ \ 0 \leq j \leq n\big\}$$

$$J_n = \big\{k \in \mathbf{N} : (a_{\phi(j)} < a_k) \Leftrightarrow (b_{\psi(j)} < b_{\psi(n+1)}),\ \ 0 \leq j \leq n\big\}$$

y definamos

$$\phi(n+1) = \begin{cases} \min F_n & \text{si } n \text{ es par y } F_n \neq \emptyset \\ \min J_n & \text{si } n \text{ es impar y } J_n \neq \emptyset \\ 0 & \text{en otro caso,} \end{cases}$$

$$\psi(n+1) = \begin{cases} \min G_n & \text{si } n \text{ es par y } G_n \neq \emptyset \\ \min H_n & \text{si } n \text{ es impar y } H_n \neq \emptyset \\ 0 & \text{en otro caso,} \end{cases}$$

Demostraremos por inducción que si $n \in \mathbf{N}$ y $j < n$, entonces
(a) $\phi(n) \neq \phi(j)$
(b) $\psi(n) \neq \psi(j)$
(c) $a_{\phi(n)} \leq a_{\phi(j)}$ si y sólo si $b_{\psi(n)} \leq b_{\psi(j)}$ y $a_{\phi(n)} \geq a_{\phi(j)}$ si y sólo si $b_{\psi(n)} \geq b_{\psi(j)}$.

Es claro que (a), (b) y (c) se cumplen para $n = 0$. Supóngase que $n_0 > 0$ y que (a), (b) y (c) se valen para $n < n_0$. Sea $n_0 = n' + 1$. La demostración ahora se parte en dos casos acorde a cuando n' es par o impar. Consideraremos únicamente el primero de los casos.

Como A es infinito, existen números k tales que $a_k \neq a_{\phi(j)}$ para $j \leq n'$. Por definición, $\phi(n'+1)$ es uno de estos números. Esto demuestra (a) para $n_0 = n' + 1$.

Para demostrar (b) y (c), sean

$$P = \left\{ j \leq n' : a_{\phi(j)} < a_{\phi(n_0)} \right\} \text{ y } Q = \left\{ j \leq n' : a_{\phi(n_0)} < a_{\phi(j)} \right\}.$$

Así, $p \in P$ y $q \in Q$ implica $a_{\phi(p)} < a_{\phi(q)}$. Por lo tanto, (c) se cumple por la suposición para $n < n'$; obteniendo con esto que

$$p \in P,\ q \in Q \ \text{ implica } \ b_{\psi(p)} < b_{\psi(q)}. \tag{11.1.1}$$

Puesto que B es denso, (11.1.1) muestra que existen números k tales que $b_{\psi(p)} < b_k$ para cualquier $p \in P$ y $b_k < b_{\psi(q)}$ para cualquier $q \in Q$. Se sigue de la definición de ψ que $\psi(n_0)$ es uno de estos números k. Así, $b_{\psi(n_0)} \neq b_{\psi(j)}$ para $j \in P \cup Q$. Más aún, $b_{\psi(n_0)} < b_{\psi(j)}$ si y sólo si $j \in Q$ si y sólo si $a_{\phi(n_0)} < a_{\phi(j)}$; y similarmente para $>$ (tomando $j \in P \cup Q$). De este modo (b) y (c) están demostradas.

f es un isomorfismo entre los conjuntos $\left\{ a_{\phi(n)} : n \in \mathbf{N} \right\}$y $\left\{ b_{\psi(n)} : n \in \mathbf{N} \right\}$ se deduce las propiedades (a), (b) y (c). Nos resta probar que estos conjuntos son idénticos con A y B, respectivamente. En otras palabras que ϕ y ψ son sobreyectivas. Consideraremos únicamente ϕ.

Supóngase por el contrario que $\mathbf{N} \setminus \phi(\mathbf{N}) \neq \emptyset$ y sea k_0 el mínimo de este conjunto. Claramente $k_0 > 0$. Para $h < k_0$, sea n_h el único número tal que $\phi(n_h) = h$ y sea n un número natural par mayor que cualquier n_h, con $h < k_0$. Como $a_{k_0} \neq a_{\phi(j)}$ para todo $j \leq n$, y para cualquier $k < k_0$ existe $j \leq n$ tal que $a_k = a_{\phi(j)}$, a saber, $j = n_k$, obtenemos que $k_0 = \min F_n$. Esto implica que $k_0 = \phi(n+1)$, lo cual contradice que $k_0 \notin \phi(N)$. ■

Definición 11.3 Sea $(A, \leq)$ un conjunto linealmente ordenado que sea denso.

(a) Decimos que $(A, \leq)$ es *completo* si cualquier subconjunto acotado no vacío de A tiene supremo.

(b) $D \subseteq A$ es *denso en* A si y sólo si para cualesquiera $a, b \in A$, existe $d \in D$ tal que $a < d < b$.

En la Sección 6.4 hicimos notar que a pesar de que los racionales son un conjunto denso, existen subconjuntos acotados no vacíos que carecen de supremo. Esta motivación nos llevo a extender el conjunto $\mathbf{Q}$ a un conjunto linealmente ordenado en el que no ocurriera este fenómeno; así construimos a $\mathbf{R}$ (por medio de clases de equivalencia de sucesiones de Cauchy). El conjunto de los números reales tiene las mismas propiedades (de orden) que $\mathbf{Q}$ y otra más, la completitud. Ahora daremos otro método de llevar a cabo esta compleción.

Definición 11.4 Una cortadura de Dedekind en un conjunto linealmente ordenado $(X, \leq)$ es un par (A, B) de subconjuntos no vacíos de X tales que:

(a) $A \cup B = X$;

(b) $a < b$ para cualesquiera $a \in A$ y $b \in B$;

(c) si $\inf B$ existe, entonces $\inf B \in B$ (note que $\sup A = \inf B$).

Teorema 11.5 *Sea $(X, \leq)$ un conjunto linealmente ordenado, denso y no acotado. Entonces existe un conjunto linealmente ordenado, completo y no acotado $(\widetilde{X}, \preceq)$ tal que:*

(a) $X \subseteq \widetilde{X}$, $\leq$ y $\preceq$ coinciden en X.

(b) X es denso en $\widetilde{X}$.

El conjunto $\widetilde{X}$ es único salvo isomorfismo; más aún, si $\widetilde{X}_1$ y $\widetilde{X}_2$ son dos de tales conjuntos entonces existe un isomorfismo h entre $\widetilde{X}_1$ y $\widetilde{X}_2$ tal que $h(a) = a$ para todo $a \in X$.

Demostración:

Sea $\widetilde{X}$ el conjunto de todas las cortaduras de Dedekind en X y sea $(A, B) \preceq (A', B')$ si y sólo si $A \subseteq A'$ (y $B \supseteq B'$). El conjunto $\widetilde{X}$ es completo. En efecto, si $\{(A_i, B_i)\}_{i \in I}$ es un subconjunto acotado de $\widetilde{X}$, entonces

$$\left(\bigcup_{i \in I} A_i, \bigcap_{i \in I} B_i \right)$$

es su supremo. Para cualquier $p \in X$, sean

$$A_p = \{x \in X : x < p\} \quad \text{y} \quad B_p = \{x \in X : x \geq p\}.$$

Entonces $X' = \{(A_p, B_p) : p \in X\}$ es isomorfo a X y es denso en $\widetilde{X}$.

Para demostrar la unicidad de $\widetilde{X}$, sean $\widetilde{X}$ y $\widetilde{X}'$ dos conjuntos linealmente ordenados, densos, completos y no acotados, sean X y X' densos en $\widetilde{X}$ y $\widetilde{X}'$, respectivamente, y sea $f : X \to X'$ un isomorfismo. Entonces f puede extenderse (unívocamente) a un isomorfismo $f^* : \widetilde{X} \to \widetilde{X}'$, haciendo

$$f^*(y) = \sup \{f(x) : x \in X,\ x \leq y\}.$$

Esto completa la demostración ■

A los conjuntos linealmente ordenados que poseen subconjuntos densos numerables se les llama *separables*. Así, por el teorema anterior, $\mathbf{R}$ es el único (salvo isomorfismo) conjunto linealmente ordenado que es denso, no acotado, completo y separable. En 1920 Souslin se preguntó si la condición de ser separable puede ser sustituida por una condición más débil.

Definición 11.6 Sea $(X, \leq)$ un conjunto linealmente ordenado. Si cada colección de intervalos abiertos ajenos es a lo más numerable, entonces se dice que X *satisface la condición de la cadena contable* (*c.c.c.*).

Claramente cualquier conjunto linealmente ordenado que sea separable satisface la condición de la cadena contable. Así, el problema de Souslin es el siguiente:

Problema de Souslin *Sea S un conjunto linealmente ordenado tal que*:

(a) S es denso y no acotado.

(b) S es completo.

(c) S satisface la condición de la cadena contable.

¿Es S isomorfo a la línea real?

Este problema no puede decidirse en la axiomática de la Teoría de Conjuntos. Jech en 1967 y Tennenbaum en 1968 descubrieron modelos en los cuales el Problema de Souslin tiene solución.

El Problema de Souslin puede reformularse como sigue: *¿Existe un conjunto linealmente ordenado S que sea denso y satisfaga la condición de la cadena contable, pero que no sea separable*?

A tales conjuntos ordenados S los llamamos *líneas de Souslin*. La Hipótesis de Souslin es la siguiente afirmación:

HS No existen líneas de Souslin.

Salvo la completitud, removiendo los puntos finales si es necesario, una línea de Souslin proporciona un contraejemplo para el problema de Souslin. Por lo tanto, la investigación se centra en la existencia de líneas de Souslin. Solovay y Tennenbaum en 1971 mostraron que la existencia de una línea de Souslin no se puede demostrar en **ZFC**; la construcción de Tennenbaum también muestra que la existencia de una línea de Souslin es independiente de la Hipótesis del Continuo y en un modelo de Jensen donde existe una línea de Souslin la Hipótesis del Continuo es válida.

Las líneas de Souslin han sido usadas en Topología de Conjuntos. Muchas de las construcciones de varios tipos de espacios no separables son imposibles en **ZFC** si no se acepta la existencia de líneas de Souslin.

11.2 El Axioma de Martin

La no existencia de una línea de Souslin puede demostrarse con el llamado *Axioma de Martin*, el cual fue estudiado e introducido por Solovay y Tennenbaum en 1971, Martin y Solovay en 1970 y Kunen en 1968. Para formularlo, introduciremos las siguientes definiciones.

Definición 11.7 Una relación $\leq$ en un conjunto P es un *pre-orden* si es reflexiva y transitiva. Al par $(P, \leq)$ le llamamos *conjunto pre-ordenado.*

Como es costumbre, abusaremos de la notación y escribiremos P en vez de $(P, \leq)$ cuando la definición del pre-orden $\leq$ sea clara dentro del contexto. También, es costumbre llamar a los elementos de un conjunto pre-ordenado P *condiciones;* y decir que una condición p *extiende* a una condición q si $p \leq q$.

Obviamente cualquier orden (parcial) es un pre-orden. Un ejemplo trivial de un pre-orden en P es $P \times P$, es decir, $p \leq q$ para cualesquiera $p, q \in P$. Otra relación $\preceq$ que es un pre-orden es la que se encuentra en el Ejemplo 4.99.

Definición 11.8 Sea P un conjunto pre-ordenado.

(a) Dos elementos $p, q \in P$ son *compatibles* si existe $r \in P$ tal que $r \leq p$ y $r \leq q$.

(b) Dos elementos $p, q \in P$ son *incompatibles* si no son compatibles.

(c) Un subconjunto $A \subseteq P$ es una *anticadena* si cualesquiera dos elementos de A son incompatibles.

(d) Un subconjunto $D \subseteq P$ es *denso* si para cualquier $p \in P$, existe $d \in D$ tal que $d \leq p$.

Es bueno observar que el concepto de compatibilidad es diferente del concepto de comparabilidad que se definió en la Sección 4.5, pues puede ocurrir

que dos condiciones p y q sean compatibles pero que no sean comparables, es decir, $p \not\leq q$ y $q \not\leq p$. También, note que aquí el uso de la palabra "denso" es diferente al uso de esta misma palabra en la sección anterior; por ejemplo, en el conjunto de los números reales con su orden usual, $(-\infty, 1)$ es un subconjunto denso según la definición anterior pero obviamente no lo es en el sentido de la Definición 11.3. Otro uso diferente al de la sección anterior, aunque con la misma terminología, es el siguiente:

Definición 11.9 Un conjunto pre-ordenado satisface la *condición de la cadena contable* (*c.c.c.*) si toda anticadena es a lo más numerable.

Note que trivialmente todo conjunto linealmente ordenado satisface la *c.c.c.* como conjunto pre-ordenado. Aquí también el peso de la tradición histórica nos obliga a llamar condición de la cadena contable a una propiedad que en realidad se refiere a anticadenas. El contexto nos permitirá distinguir con claridad a cuál *c.c.c.* nos referimos.

Ejemplo 11.10 Sean X un conjunto no vacío y $P = \mathcal{P}(X) \setminus \{\emptyset\}$ con $p \leq q$ si y sólo si $p \subseteq q$. Entonces dos condiciones p y q son incompatibles si y sólo si $p \cap q = \emptyset$. $A \subseteq P$ es una anticadena si sus elementos son ajenos por pares; así, P satisface la *c.c.c.* si y sólo si $|X| \leq \aleph_0$.

Ejemplo 11.11 Sea (X, τ) un espacio topológico y

$$P = \{p \subseteq X : p \neq \emptyset,\ p \text{ es abierto en } X\}. \tag{11.2.1}$$

Como en el ejemplo anterior, sea $\leq$ la contención de conjuntos. Entonces $p, q \in P$ son incompatibles si y sólo si $p \cap q = \emptyset$.

Si $(X, \leq)$ es un conjunto linealmente ordenado, una topología sobre X puede ser introducida declarando como abiertos a todos los subconjuntos de X que sean unión de intervalos abiertos. X con esta topología $\tau_{\leq}$, $(X, \tau_{\leq})$, se llama espacio linealmente ordenado. $(X, \leq)$ satisface la *c.c.c.,* según la Definición 11.6, si y sólo si el conjunto pre-ordenado P definido en el ejemplo anterior satisface la *c.c.c.* según la Definición 11.9. Más generalmente, se dice que un espacio topológico (X, τ) *satisface la c.c.c. si el conjunto pre-ordenado (11.2.1) satisface la c.c.c.* (según la Definición 11.9).

Ejemplo 11.12 Sean B un álgebra booleana y $P = B \setminus \{0\}$, con el mismo orden como en B. Entonces dos condiciones p y q son incompatibles si y sólo si $p \cdot q = 0$.

Definición 11.13 Si D es un subconjunto denso de un conjunto pre-ordenado P, entonces un subconjunto G de P se llama *filtro D-genérico* en P si satisface las siguientes condiciones:

(a) si $a \in G$ y $a \leq b$ entonces $b \in G$,

(b) si $a, b \in G$ entonces existe $c \in G$ tal que $c \leq a$ y $c \leq b$,

(c) $D \cap G \neq \emptyset$.

Si $\mathcal{D}$ es una familia de conjuntos densos en P, entonces G es un *filtro $\mathcal{D}$-genérico* si es un filtro D-genérico para cada $D \in \mathcal{D}$.

Lema 11.14 *Si $(P, \leq)$ es un conjunto ordenado, y $\mathcal{D}$ es una familia a lo más numerable de subconjuntos densos de P, entonces existe un filtro $\mathcal{D}$-genérico en P. En efecto, para cualquier $p \in P$, existe un filtro $\mathcal{D}$-genérico G en P tal que $p \in G$.*

Demostración:

Sea $\mathcal{D} = \{D_1, D_2, \ldots\}$ una familia numerable de conjuntos densos en P. Sean p un elemento cualquiera de P y $p_0 = p$. Para cada $n > 0$, sea p_n tal que $p_n \leq p_{n-1}$ y $p_n \in D_n$. Veamos que el conjunto

$$G = \{x \in P : x \geq p_n \text{ para algún } n \in \mathbf{N}\}$$

es un filtro $\mathcal{D}$-genérico en P y que $p \in G$. En efecto, que $p \in G$ es claro. Ahora si $r \in P$, $q \in G$ y $q \leq r$; entonces $r \in G$ (puesto que $q \in G$ implica la existencia de un $n \in \omega$ tal que $p_n \leq q$). Además, si $q_1, q_2 \in G$ existen $m, n \in \omega$ tales que $p_m \leq q_1$ y $p_n \leq q_2$. Sin pérdida de generalidad supongamos que $m \leq n$. Entonces $p_m \in G$ es una extensión común a q_1 y q_2. Finalmente, es obvio que $G \cap D_n \neq \emptyset$ para todo $n \in \omega$. ■

Consideremos la siguiente generalización.

$\mathbf{AM}_\kappa$ Si κ es un cardinal infinito y $(P, \leq)$ es un conjunto pre-ordenado que satisface la condición de la cadena contable, y si $\mathcal{D}$ es una familia de a lo más κ subconjuntos densos de P, entonces existe un filtro $\mathcal{D}$-genérico en P.

$\mathbf{AM}_{\aleph_0}$ es justamente el Lema 11.14 y es demostrable en **ZFC**. El Axioma de Martin asegura que **$\mathbf{AM}_\kappa$** se cumple para todo $\kappa < 2^{\aleph_0}$.

Axioma de Martin Si $(P, \leq)$ es un conjunto pre-ordenado que satisface la condición de la cadena contable y si $\mathcal{D}$ es una colección de menos que $2^{\aleph_0}$ subconjuntos densos de P, entonces existe un filtro $\mathcal{D}$-genérico en P.

Como $\mathbf{AM}_{\aleph_0}$ siempre es cierto, se sigue que el Axioma de Martin (**AM**) es una consecuencia de la Hipótesis del Continuo. El Axioma de Martin intuitivamente nos dice que los cardinales que se encuentran entre $\aleph_0$ y $2^{\aleph_0}$ tienen el "mismo comportamiento" que $\aleph_0$, lo cual permite reemplazar a la Hipótesis del Continuo en numerosas demostraciones que hacen uso de ella; esto es importante puesto que el Axioma de Martin puede cumplirse aun cuando la Hipótesis del Continuo falle. También, con frecuencia, una proposición que es cierta asumiendo la Hipótesis del Continuo puede resultar falsa asumiendo el Axioma de Martin. Puesto que el Axioma de Martin más la negación de la Hipótesis del Continuo es consistente con los axiomas **ZFC**, cualesquiera de tales proposiciones es en sí misma independiente de **ZFC**.

Para empezar nuestro estudio del Axioma de Martin analizaremos un tipo de conjunto pre-ordenado que es muy empleado para distintas aplicaciones de **AM**; en esta ocasión nos aclarará por qué se pide $|\mathcal{D}| < 2^{\aleph_0}$ en su formulación.

Sea $P = \bigcup_{n\in\omega} 2^n$ (el conjunto de todas las sucesiones finitas de ceros y unos). Para $p, q \in P$ definimos $p \leq q$ si y sólo si $dom\, p \supseteq dom\, q$ y p es una extensión (como función) de q. Entonces p y q son compatibles si y sólo si para cualquier $n \in (dom\, p) \cap (dom\, q)$ se tiene que $p(n) = q(n)$, es decir, son compatibles como funciones. Puesto que $|P| = \aleph_0$, P satisface la *c.c.c.*

Ahora, sea $\mathcal{D} = \{D_h : h \in 2^\omega\} \cup \{E_n : n \in \omega\}$, donde para cada $h \in 2^\omega$,

$$D_h = \{p \in P : p \neq h\,|_{dom\, p}\},$$

y para cada $n \in \omega$,

$$E_n = \{p \in P : n \in dom\, p\}. \tag{11.2.2}$$

Cada E_n es un subconjunto denso en P: si $p \in P$ y $n \notin dom\, p$, basta definir $q : dom\, p \cup \{n\} \to 2$ como $q(k) = p(k)$ para cada $k \in dom\, p$ y $q(n) = 0$; así, $q \leq p$ y $q \in E_n$. También cada D_h es un subconjunto denso en P: si $p \in P \setminus D_h$ y $n \notin dom\, p$, claramente podemos tomar $q \in E_n$ tal que $q \leq p$ y $q(n) \neq h(n)$; entonces $q \in D_h$ y $q \leq p$.

Supongamos que G es un filtro $\mathcal{D}$-genérico en P; entonces, en virtud de la condición (b) de la Definición 11.8, G es un sistema compatible de funciones, y en virtud de la condición (c) de la misma definición,

$$f = \bigcup G : \omega \to 2$$

es una función. Además, si $h : \omega \to 2$ es cualquier función, dado que existen $p \in G \cap D_n$ y $n \in dom\, p$ tales que $p(n) \neq h(n)$, como $f(n) = p(n)$ se sigue que $f \neq h$. En resumen, $f \in 2^\omega$ pero, para cualquier $h \in 2^\omega$, $f \neq h$; lo cual es imposible. Hemos demostrado entonces la siguiente proposición.

Proposición 11.15 $\mathbf{AM}_{2^{\aleph_0}}$ *es falsa.*

Corolario 11.16 $\mathbf{AM}_{\aleph_1}$ *implica que la Hipótesis del Continuo es falsa.*

Un resultado inmediato es el comportamiento de $\mathbf{AM}_\kappa$ para distintos κ.

Proposición 11.17 *Si* $\aleph_0 < \kappa < \kappa' < 2^{\aleph_0}$*, entonces* $\mathbf{AM}_{\kappa'}$ *implica* $\mathbf{AM}_\kappa$*.*

El Lema 11.14 no necesita en absoluto que P satisfaga la *c.c.c.* y uno estaría tentado a fortalecer $\mathbf{AM}_\kappa$ quitando este requerimiento. No obstante, como veremos a continuación, para $\kappa > \aleph_0$ este fortalecimiento se vuelve inconsistente.

Ejemplo 11.18 Sea $P = \bigcup_{n\in\omega}(\omega_1)^n$ (el conjunto de todas las sucesiones finitas de ω en ω_1). Para $p, q \in P$ definimos $p \leq q$ si y sólo si $p \subseteq q$. Para cada $\alpha \in \omega_1$ sea

$$D_\alpha = \{p \in P : \alpha \in ran\, p\}\,.$$

Entonces cada D_α es denso en P. Supongamos que P satisface la *c.c.c.* Sea $\mathcal{D} = \{D_\alpha : \alpha < \omega_1\}$. A partir de $\mathbf{AM}_{\aleph_1}$ podemos inferir la existencia de un filtro $\mathcal{D}$-genérico G. Entonces $f = \bigcup G$ es una función con dominio contenido en ω y $ran\, f = \omega_1$. Pero esto es imposible. Por lo tanto, no es posible omitir la *c.c.c.* en $\mathbf{AM}_{\aleph_1}$ (y por tanto, en $\mathbf{AM}_\kappa$ para cualquier $\aleph_0 < \kappa < 2^{\aleph_0}$).

Hasta aquí puede considerarse la discusión elemental del Axioma de Martin. Procederemos ahora a dar una breve muestra de cómo aplicar **AM.**

Definición 11.19 Una familia $\mathcal{A} \subseteq \mathcal{P}(\omega)$ se llama *casi ajena* si cualquiera de sus miembros es infinito y para cualesquiera dos distintos $A, B \in \mathcal{A}$ se tiene que $|A \cap B| < \aleph_0$.

Ejemplo 11.20 Si $\mathcal{A}$ consiste únicamente del conjunto de números naturales pares y del conjunto de los números naturales impares, entonces $\mathcal{A}$ es casi ajena. Más generalmente, cualquier familia ajena por pares es una familia casi ajena.

Ejemplo 11.21 Para cada $r \in \mathbf{R}$ existe una sucesión $(a_n^{(r)})_{n\in\omega}$ de números racionales que converge a r. Sean $f : \omega \to \mathbf{Q}$ una función biyectiva y

$$A_r = \left\{k \in \omega : \exists n \in \omega,\ f(k) = a_n^{(r)}\right\},$$

para cada $r \in \mathbf{R}$. Entonces $\mathcal{A} = \{A_r : r \in \mathbf{R}\}$ es una familia casi ajena de cardinalidad $2^{\aleph_0}$.

Definición 11.22 $\mathcal{A} \subseteq \mathcal{P}(\omega)$ es una *familia casi ajena maximal* si no existe una familia casi ajena $\mathcal{B}$ tal que $\mathcal{B} \supset \mathcal{A}$.

Usando el Lema de Kuratowski-Zorn puede demostrarse que siempre que $\mathcal{A}$ sea una familia casi ajena, existe una familia casi ajena maximal $\mathcal{B}$ tal que $\mathcal{A} \subseteq \mathcal{B}$. El Ejemplo 11.20 muestra una familia casi ajena maximal finita; aplicaremos **AM** para investigar la cardinalidad de una familia casi ajena maximal infinita.

Proposición 11.23 *No existe una familia casi ajena maximal de cardinalidad* $\aleph_0$.

Demostración:

Sean $\mathcal{A} = \{A_n : n \in \omega\}$ una familia casi ajena y $B_n = A_n \setminus \bigcup_{m<n} A_m$, para cada $n \in \omega$. $B_n \neq \emptyset$ puesto que $B_n = A_n \setminus \bigcup_{m<n}(A_n \cap A_m)$, $|A_n| = \aleph_0$ y $\left|\bigcup_{m<n}(A_n \cap A_m)\right| < \aleph_0$. Elijamos $k_n \in B_n$ para cada $n \in \omega$. Los k_n son distintos ya que los B_n son ajenos, así $D = \{k_n : n \in \omega\}$ es infinito y además si $k_n \in A_m$ entonces $m \geq n$; con esto $D \cap A_m \subseteq \{k_n : n < m\}$. Por lo tanto, $\mathcal{B} = \mathcal{A} \cup \{D\}$ es una familia casi ajena que contiene propiamente a $\mathcal{A}$. ■

Si suponemos la Hipótesis del Continuo, claramente la cardinalidad de una familia casi ajena maximal debe ser $2^{\aleph_0}$. **AM** nos ayudará a ver qué ocurre en caso de que existan cardinales mayores que $\aleph_0$ y menores que $2^{\aleph_0}$. Para esto introduciremos un nuevo conjunto pre-ordenado.

Definición 11.24 Para $\mathcal{A} \subseteq \mathcal{P}(\omega)$ sea

$$P_{\mathcal{A}} = \left\{(s, F) : s \in [\omega]^{<\aleph_0},\ F \in [\mathcal{A}]^{<\aleph_0}\right\},$$

y dados (s_1, F_1), $(s_2, F_2) \in P_{\mathcal{A}}$ definimos $(s_1, F_1) \leq (s_2, F_2)$ si y sólo si

$$s_2 \subseteq s_1,\ F_2 \subseteq F_1 \ y\ \forall x \in F_2,\ x \cap s_1 \subseteq s_2.$$

La intención de las condiciones $(s, F) \in P_{\mathcal{A}}$ es describir un $d \subseteq \omega$ que es casi ajeno (es decir, tiene intersección finita) con los elementos de $\mathcal{A}$; (s, F) "fuerza" a que $s \subseteq d$ y para cualquier $x \in F$, $d \cap x \subseteq s$; así, (s, F) "fuerza" $n \notin d$ siempre que $n \in x \setminus s$ para algún $x \in F$.

Dos condiciones $(s_1, F_1), (s_2, F_2) \in P_{\mathcal{A}}$ son compatibles si y sólo si para todo $x \in F_1$, $x \cap s_2 \subseteq s_1$ y para todo $x \in F_2$, $x \cap s_1 \subseteq s_2$. Si éste es el caso $(s_1 \cup s_2, F_1 \cup F_2)$ es una extensión común.

$P_{\mathcal{A}}$ satisface la *c.c.c.* pues si $\{(s_\xi, F_\xi) : \xi < \omega_1\}$ fuera una anticadena, entonces $s_\xi \neq s_{\xi'}$ para cada $\xi \neq \xi'$, que es imposible.

Ahora si G es un filtro (es decir, satisface (a) y (b) de la Definición 11.8) en $P_{\mathcal{A}}$ se define

$$d_G = \bigcup \{s : \exists F \in \mathcal{A},\ (s,F) \in G\}. \tag{11.2.3}$$

Entonces, si G es un filtro en $P_{\mathcal{A}}$ y $(s,F) \in G$, necesariamente para todo $x \in F,\ x \cap d_G \subseteq s$. En efecto, si $(s',F') \in G$, entonces (s,F) y (s',F') son compatibles. Así, para todo $x \in F,\ x \cap s' \subseteq s$; lo cual implica $x \cap d_G \subseteq s$.

Para $x \in \mathcal{A}$ definimos

$$D_x = \{(s,F) \in P_{\mathcal{A}} : x \in F\}. \tag{11.2.4}$$

Entonces D_x es denso en $P_{\mathcal{A}}$ para cada $x \in \mathcal{A}$, pues si $(s,F) \in P_{\mathcal{A}}$,

$$(s, F \cup \{x\}) \leq (s,F).$$

También, si G es un filtro en $P_{\mathcal{A}}$ y $G \cap D_x \neq \emptyset$, entonces $|x \cap d_G| < \aleph_0$ puesto que $x \cap d_G \subseteq s$ y $|s| < \aleph_0$. Sin embargo, d_G puede ser finito e incluso vacío; porque si existiera algún $F \subseteq \mathcal{A}$ tal que $\omega \setminus \bigcup F$ fuera finito, entonces ningún d infinito podría ser casi ajeno a todos los elementos de F.

A continuación se demostrará que si no existe F tal que $\omega \setminus \bigcup F$ es finito, entonces podemos hacer que d sea infinito. Más generalmente, podemos hacer que d tenga intersección infinita con cualquier subconjunto de ω el cual no está casi cubierto (es decir, a excepción de una cantidad finita de elementos) por una unión finita de elementos de $\mathcal{A}$.

Teorema 11.25 *Sean $\mathcal{A}, \mathcal{C} \subseteq \mathcal{P}(\omega)$ tales que $|\mathcal{A}| \leq \kappa,\ |\mathcal{C}| \leq \kappa$ y, para cada $y \in \mathcal{C}$ y cada $F \subseteq \mathcal{A}$,*

$$|F| \leq \aleph_0 \Rightarrow \left| y \setminus \bigcup F \right| = \aleph_0.$$

Entonces $\mathbf{AM}_\kappa$ implica que existe $d \in \mathcal{P}(\omega)$ tal que

$$\forall x \in \mathcal{A},\ |d \cap x| < \aleph_0 \quad \text{y} \quad \forall y \in \mathcal{C},\ |d \cap y| = \aleph_0.$$

Demostración:

Para $y \in \mathcal{C}$ y $n \in \omega$ sea

$$E^y_n = \{(s,F) \in P_{\mathcal{A}} : s \cap y \nsubseteq n\}.$$

E^y_n es denso en $P_{\mathcal{A}}$ ya que para cada $(s,F) \in P_{\mathcal{A}}$, $|y \setminus \bigcup F| = \aleph_0$; si tomamos $m \in y \setminus \bigcup F$ con $m > n$, entonces $(s \cup \{m\}, F) \in E^y_n$ es una extensión de (s,F).

Sea

$$\mathcal{D} = \{D_x : x \in \mathcal{A}\} \cup \{E^y_n : y \in \mathcal{C},\ n \in \omega\},$$

donde los conjuntos D_x son los que se definieron en (11.2.4). Por $\mathbf{AM}_\kappa$, hay un filtro $\mathcal{D}$-genérico G. Ya hemos visto que si d_G es como en (11.2.3), entonces $d_G \cap x$ es finito para cada $x \in \mathcal{A}$. Si $y \in \mathcal{C}$, entonces $d_G \cap y \nsubseteq n$ para todo $n \in \omega$, ya que $G \cap E^y_n \neq \emptyset$ para cada $n \in \omega$. Por lo cual concluimos que $d_G \cap y$ es infinito. ■

Corolario 11.26 *Sea $\mathcal{A} \subseteq \mathcal{P}(\omega)$ una familia casi ajena de cardinalidad κ, donde $\aleph_0 \leq \kappa < 2^{\aleph_0}$. Suponiendo $\mathbf{AM}_\kappa$ se tiene que $\mathcal{A}$ no es maximal.*

Demostración:

Sea $\mathcal{C} = \{\omega\}$ y sea $F \in \mathcal{A}$ finito. Puesto que $|\mathcal{A}| = \kappa$, podemos tomar $B \in \mathcal{A} \setminus F$. Como $\mathcal{A}$ es casi ajena, $|B \cap \bigcup F| < \aleph_0$. Así, $|B \cap (\omega \setminus \bigcup F)| = \aleph_0$; y esto implica que $|\omega \setminus \bigcup F| = \aleph_0$. El teorema anterior garantiza que existe $d \subseteq \omega$ infinito y casi ajeno a cada elemento de $\mathcal{A}$. ■

Corolario 11.27 *Sea $\mathcal{B} \subseteq \mathcal{P}(\omega)$ una familia casi ajena de cardinalidad κ, donde $\aleph_0 \leq \kappa < 2^{\aleph_0}$. Si $\mathcal{A} \subseteq \mathcal{B}$ y si suponemos $\mathbf{AM}_\kappa$, entonces existe $d \subseteq \omega$ tal que para cada $x \in \mathcal{A}$, $|d \cap x| < \aleph_0$ y para cada $x \in \mathcal{B} \setminus \mathcal{A}$, $|d \cap x| = \aleph_0$.*

Demostración:

Aplicar el teorema anterior a $\mathcal{C} = \mathcal{B} \setminus \mathcal{A}$. ■

Teorema 11.28 *Si $\aleph_0 \leq \kappa < 2^{\aleph_0}$, $\mathbf{AM}_\kappa$ implica que $2^\kappa = 2^{\aleph_0}$.*

Demostración:

Sea $\mathcal{B}$ una familia casi ajena de cardinalidad κ. Definamos $\Phi : \mathcal{P}(\omega) \to \mathcal{P}(\mathcal{B})$ por

$$\Phi(d) = \{x \in \mathcal{B} : |d \cap x| < \aleph_0\}.$$

El corolario anterior implica que Φ es sobreyectiva; así,

$$2^\kappa = |\mathcal{P}(\mathcal{B})| \leq |\mathcal{P}(\omega)| = 2^{\aleph_0}. \quad ■$$

Corolario 11.29 **AM** *implica que $2^{\aleph_0}$ es regular.*

DEMOSTRACIÓN:

Sea $\kappa < 2^{\aleph_0}$. Por la Proposición 10.29 tenemos que $\kappa < cf(2^\kappa)$. Además, **AM** implica que $2^\kappa = 2^{\aleph_0}$, lo cual significa que $\kappa < cf(2^{\aleph_0})$. Por lo tanto, $cf(2^{\aleph_0}) = 2^{\aleph_0}$. ■

Es consistente con **ZFC** que $2^{\aleph_0}$ sea un cardinal singular, tal como $\aleph_{\omega_1}$; pero, como vimos en la Proposición 10.29, $cf(2^{\aleph_0}) > \aleph_0$.

De la siguiente aplicación de **AM** a la topología se decidirá el problema de Souslin.

Lema 11.30 *Supongamos* $\mathbf{AM}_{\aleph_1}$. *Si X es un espacio topológico que satisface la c.c.c. y $\{U_\alpha : \alpha < \omega_1\}$ es una familia de subconjuntos abiertos no vacíos, entonces existe $A \subseteq \omega_1$ no numerable tal que $\{U_\alpha : \alpha \in A\}$ tiene la propiedad de la intersección finita.*

DEMOSTRACIÓN:

Sea $V_\alpha = \bigcup_{\gamma>\alpha} U_\gamma$. Entonces $\alpha < \beta$ implica $V_\beta \subseteq V_\alpha$. Veamos primero que existe α tal que para todo $\beta > \alpha$,

$$\overline{V}_\beta = \overline{V}_\alpha. \tag{11.2.5}$$

Si no hay tal α podríamos encontrar una sucesión creciente de ordinales $(\alpha_\xi)_{\xi\in\omega_1}$ tal que para cada ξ, $\overline{V}_{\alpha_{\xi+1}} \neq \overline{V}_{\alpha_\xi}$, con lo cual, $V_{\alpha_\xi} \setminus \overline{V}_{\alpha_{\xi+1}} \neq \emptyset$. Entonces

$$\left\{V_{\alpha_\xi} \setminus \overline{V}_{\alpha_{\xi+1}} : \xi < \omega_1\right\}$$

sería una familia de abiertos no vacíos ajena por pares contradiciendo que X satisface la *c.c.c.*

Ahora fijemos α de tal forma que satisfaga la ecuación (11.2.5) y sea

$$P = \{p \subseteq V_\alpha : p \text{ es abierto y } p \neq \emptyset\}$$

con el pre-orden $p \leq q$ si y sólo si $p \subseteq q$. Entonces P satisface la *c.c.c.* porque X la satisface y V_α es abierto. Para cada $\beta < \omega_1$, sea

$$D_\beta = \{p \in P : \exists\gamma > \beta,\ p \subseteq U_\gamma\}.$$

Entonces cada D_β es denso en P. En efecto, por (11.2.5), $\overline{V}_\alpha \subseteq \overline{V}_\beta$; así, si $p \in P$ entonces $p \cap V_\beta \neq \emptyset$ con lo cual $p \cap U_\gamma \neq \emptyset$ para algún $\gamma > \beta$ y de aquí que $p \cap U_\gamma$ es una extensión de p en D_β.

Sea $\mathcal{D} = \{D_\beta : \beta < \omega_1\}$. Por $\mathbf{AM}_{\aleph_1}$, existe un filtro $\mathcal{D}$-genérico G. Pongamos

$$A = \{\gamma < \omega_1 : \exists p \in G,\ p \subseteq U_\gamma\}.$$

Como G es un filtro, G tiene la propiedad de la intersección finita y entonces también $\{U_\gamma : \gamma \in A\}$ tiene la propiedad de la intersección finita. Más aún, para cada $\beta < \omega_1$, A debe contener algún $\gamma > \beta$, ya que $G \cap D_\beta \neq \emptyset$. Esto implica que A es no acotado en ω_1 y por lo tanto, $|A| = \aleph_1$. ■

Teorema 11.31 *Supongamos* $\mathbf{AM}_{\aleph_1}$. *Si X y Y son espacios topológicos que satisfacen la c.c.c., entonces $X \times Y$ también satisface la c.c.c.*

Demostración:

Supongamos que $X \times Y$ no satisface la *c.c.c.* Sea

$$\{W_\alpha : \alpha < \omega_1\}$$

una familia ajena por pares de subconjuntos abiertos no vacíos de $X \times Y$. Para cada α seleccionemos $U_\alpha \times V_\alpha \subseteq W_\alpha$ con $U_\alpha \neq \emptyset \neq V_\alpha$. Por el lema anterior, sea $A \subseteq \omega_1$ no numerable tal que $\{U_\alpha : \alpha \in A\}$ tiene la propiedad de la intersección finita. Si $\alpha, \beta \in A$ y $\alpha \neq \beta$, entonces $U_\alpha \cap U_\beta \neq \emptyset$; pero

$$(U_\alpha \times V_\alpha) \cap (U_\beta \cap V_\beta) = \emptyset;$$

así que $V_\alpha \cap V_\beta = \emptyset$. Entonces $\{V_\alpha : \alpha \in A\}$ contradice que Y satisface la *c.c.c.* ■

Si X es una línea de Souslin, X puede considerarse un espacio topológico linealmente ordenado (es decir, con la topología inducida por su relación de orden). Obviamente, X como espacio topológico satisface la *c.c.c.* pero no es separable (ver Ejemplo 11.11 y el comentario posterior).

Lema 11.32 *Si X es una línea de Souslin, entonces $X \times X$ no satisface la c.c.c.*

Demostración:

Si $a, b \in X$ y $a < b$; (a, b) denotará el intervalo abierto $\{x \in X : a < x < b\}$. El conjunto (a, b) puede ser vacío.

Por inducción sobre α, se encontrarán a_α, b_α, y c_α tales que:

(1) $a_\alpha < b_\alpha < c_\alpha$,

(2) $(a_\alpha, b_\alpha) \neq \emptyset$ y $(b_\alpha, c_\alpha) \neq \emptyset$,

(3) $(a_\alpha, c_\alpha) \cap \{b_\xi : \xi < \alpha\} = \emptyset$.

Sea W el conjunto de puntos aislados de X. Como X satisface la *c.c.c.* $|W| \leq \aleph_0$. Ahora, supongamos que se han elegido $a_\xi,\ b_\xi,\ c_\xi$ para $\xi < \alpha$. Como X no es separable

$$X \setminus cl\,(W \cup \{b_\xi : \xi < \alpha\})$$

es abierto y no vacío; así, contiene un intervalo abierto no vacío (a_α, c_α). Como (a_α, c_α) no tiene puntos aislados es infinito. Sea $b_\alpha \in (a_\alpha, c_\alpha)$ tal que $(a_\alpha, b_\alpha) \neq \emptyset$ y $(b_\alpha, c_\alpha) \neq \emptyset$.

Finalmente, sea $U_\alpha = (a_\alpha, b_\alpha) \times (b_\alpha, c_\alpha)$. Por (2) $U_\alpha \neq \emptyset$ para cada α. Si $\xi < \alpha$, entonces $U_\xi \cap U_\alpha = \emptyset$ ya que por (3) o bien $b_\xi < a_\xi$ y en tal caso $(a_\xi, b_\xi) \cap (a_\alpha, b_\alpha) = \emptyset$, o $b_\xi \geq c_\alpha$ y en tal caso $(b_\xi, c_\xi) \cap (b_\alpha, c_\alpha) = \emptyset$. Así,

$$\{U_\alpha : \alpha < \omega_1\}$$

impide que $X \times X$ satisfaga la *c.c.c.* ■

Corolario 11.33 $\mathbf{AM}_{\aleph_1}$ *implica* **HS.**

Demostración:

$\mathbf{AM}_{\aleph_1}$ implica que el producto de espacios que satisfacen la *c.c.c.* satisface la *c.c.c.* Por lo tanto, el corolario se sigue del lema anterior y el Teorema 11.31. ■

Otra aplicación más del Axioma de Martin a la Topología es el Teorema 11.34 que exponemos a continuación. Observe que para $\kappa = \aleph_0$, el Teorema 11.34 es conocido como el Teorema de Baire que puede ser demostrado
(como el Lema 11.14) a partir de los axiomas **ZFC** y sin requerir la *c.c.c.*

Teorema 11.34 *Supongamos* $\mathbf{AM}_\kappa$*. Si X es un espacio compacto Hausdorff que satisface la c.c.c. y $\{U_\alpha : \alpha < \kappa\}$ es una familia de conjuntos abiertos densos en X, entonces*

$$\bigcap \{U_\alpha : \alpha < \kappa\} \neq \emptyset.$$

Demostración:

Sea $P = \{p \subseteq X : p \text{ es abierto y } p \neq \emptyset\}$ con $p \leq q$ si y sólo si $p \subseteq q$. Entonces P satisface la *c.c.c.* puesto que X satisface la *c.c.c.* (ver Ejemplo 11.11 y el comentario posterior). Para cada $\alpha < \kappa$, sean

$$D_\alpha = \{p \in P : \overline{p} \subseteq U_\alpha\}$$

y $\mathcal{D} = \{D_\alpha : \alpha < \kappa\}$. Vamos a demostrar que cada D_α es denso en P. Sea $q \in P$ cualquiera. Como U_α es denso en el espacio X, $U_\alpha \cap q \neq \emptyset$. Sea $x \in U_\alpha \cap q$.

Puesto que X es Hausdorff y compacto, $K = X\backslash(U_\alpha \cap q)$ es compacto. Además, $x \notin K$; entonces existe $p \in P$ tal que $x \in p$ y $\overline{p} \cap K = \emptyset$. Consecuentemente, $p \leq q$ y $p \in D_\alpha$. Por lo tanto, D_α es denso en P. Si G es un filtro $\mathcal{D}$-genérico en P, entonces G tiene la propiedad de la intersección finita y así por la compacidad

$$\bigcap \{\overline{p} : p \in G\} \neq \emptyset.$$

Pero $\bigcap \{\overline{p} : p \in G\} \subseteq \bigcap \{U_\alpha : \alpha < \kappa\}$. Esto demuestra el teorema. ■

11.3 Equivalencias del Axioma de Martin

Aunque hay numerosas equivalencias del Axioma de Martin, en esta sección presentaremos dos de las más importantes: la topológica y la que se expresa en términos de álgebras booleanas. Empezaremos por demostrar que es posible restringir $\mathbf{AM}_\kappa$ a conjuntos pre-ordenados de cardinalidad menor o igual a κ.

Definición 11.35 Denotaremos por $\mathbf{AM}^*_\kappa$ a la proposición: Si $(P, \leq)$ es un conjunto pre-ordenado de cardinalidad menor o igual a κ, que satisface la c.c.c. y $\mathcal{D}$ es una familia de a lo más κ subconjuntos densos en P, entonces existe un filtro $\mathcal{D}$-genérico en P.

Lema 11.36 *Sea A un conjunto. Si $\{f_\alpha \in A^A : \alpha < \kappa\}$ es una familia de funciones y $g : A \times A \to A$, entonces existe $B \subseteq A$ con $|B| \leq \kappa$, $g(B \times B) \subseteq B$ y $f_\alpha(B) \subseteq B$ para cada $\alpha < \kappa$. En este caso se dice que B es cerrado respecto a la familia $\{f_\alpha\}_{\alpha \in I} \cup \{g\}$.*

Demostración:

Sean $a \in A, C_0 = \{a\}$ y

$$C_{n+1} = C_n \cup g(C_n \times C_n) \cup \bigcup_{\alpha < \kappa} f(C_n).$$

Ya que la cardinalidad de la imagen de un conjunto bajo una función no excede la cardinalidad de dicho conjunto, sin dificultad se demuestra, por inducción sobre n, que $|C_n| \leq \kappa$ para todo $n \in \omega$. Si hacemos $B = \bigcup_{n \in \omega} C_n$, entonces $|B| \leq \kappa$, $g(B \times B) \subseteq B$ y $f_\alpha(B) \subseteq B$ para todo $\alpha < \kappa$. ■

Teorema 11.37 *Para cualquier $\kappa < 2^{\aleph_0}$, $\mathbf{AM}_\kappa$ es equivalente a $\mathbf{AM}^*_\kappa$.*

DEMOSTRACIÓN:

Que $\mathbf{AM}_\kappa$ implica $\mathbf{AM}^*_\kappa$ es trivial. Supongamos $\mathbf{AM}^*_\kappa$ y sean $(Q, \leq)$ un conjunto pre-ordenado que satisfaga la *c.c.c.* y $\mathcal{D} = \{D_\alpha : \alpha < \kappa\}$ una familia de conjuntos densos en Q.

Para cada $\alpha < \kappa$, sea $f_\alpha : Q \to Q$ tal que $f_\alpha(p) \in D_\alpha$ y $f_\alpha(p) \leq p$ para cada $p \in Q$. Estos f_α existen debido a la densidad de D_α. Sea $g : Q \times Q \to Q$ tal que para cualesquiera $p, q \in Q$,

$$p \text{ y } q \text{ compatibles } \Rightarrow g(p,q) < p \text{ y } g(p,q) \leq q.$$

Existe $P \subseteq Q$ de cardinalidad no mayor a κ y que es cerrado respecto a la familia $\{f_\alpha : \alpha < \kappa\} \cup \{g\}$. Entonces:

(1) Para cada $\alpha < \kappa,\ D_\alpha \cap P \neq \emptyset$ y es denso en P,

(2) P satisface la *c.c.c.*

Aplicando $\mathbf{AM}^*_\kappa$, existe un filtro $\mathcal{D}$-genérico G en P. G puede no ser $\mathcal{D}$-genérico en Q; pero

$$H = \{q \in Q : \exists p \in G,\ p \leq q\}$$

sí es un filtro $\mathcal{D}$-genérico en Q. ■

Recordemos que si B es un álgebra booleana hay un orden natural en B inducido por las operaciones binarias de B. A este orden nos referiremos a continuación.

Definición 11.38 Un álgebra booleana B es *completa* si para cualquier $A \subseteq B$, no vacío, existe el supremo de A.

De manera más o menos corriente se demuestra que si cada subconjunto no vacío de B tiene supremo, entonces cada subconjunto no vacío de B tiene ínfimo.

Ejemplo 11.39 Sean X un espacio topológico y

$$B = \{U \subseteq X : U \text{es abierto regular}\}.^1$$

[1] U es abierto regular si $U = int(\overline{U})$.

Para $U, V \in B$ sean:

$$\begin{aligned} U \cdot V &= U \cap V \\ U + V &= int(\overline{U \cup V}) \\ -U &= int(X \setminus U) \\ 0 &= \emptyset \\ 1 &= X \end{aligned}$$

Entonces B es un álgebra booleana completa y para cada $C \in \mathcal{P}(B) \setminus \{\emptyset\}$,

$$\sup C = int(\overline{\bigcup C}) \quad y \quad \inf C = int(\bigcap C).$$

Para aplicaciones al Axioma de Martin no estaremos interesados en B sino en $B \setminus \{0\}$. Abusaremos de notación y diremos que una anticadena en B es un conjunto $A \subseteq B \setminus \{0\}$ tal que para cualesquiera $a, b \in A$,

$$a \neq b \Rightarrow a \cdot b = 0$$

(A realmente es una anticadena en $B \setminus \{0\}$). Decimos que B satisface la *c.c.c.* si y sólo si todas las anticadenas en B son a lo más numerables. Sea $\mathcal{D}$ una familia de conjuntos densos en $B \setminus \{0\}$. Por un filtro $\mathcal{D}$-genérico en B entenderemos un $G \subseteq B \setminus \{0\}$, el cual es un filtro, en el sentido usual para álgebras booleanas (ver Definición 8.46), que intersecta a cada elemento de $\mathcal{D}$. No es difícil ver que esta noción coincide con la dada en la Definición 11.8.

Definición 11.40 Denotaremos por $\mathbf{AM}^b_\kappa$ a la proposición: Si B es un álgebra booleana completa y que satisface la c.c.c. y $\mathcal{D}$ es una familia de a lo más κ subconjuntos densos en B, entonces existe un filtro $\mathcal{D}$-genérico en B.

Teorema 11.41 *Para cualquier $\kappa < 2^{\aleph_0}$, $\mathbf{AM}_\kappa$ es equivalente a $\mathbf{AM}^b_\kappa$.*

Demostración:

Es trivial que $\mathbf{AM}_\kappa$ implica $\mathbf{AM}^b_\kappa$. Supongamos $\mathbf{AM}^b_\kappa$ y sea P un conjunto pre-ordenado de cardinalidad menor o igual a κ. Para cada $p \in P$, sea

$$N_p = \{q \in P : q \leq p\}.$$

Entonces, dado que para cada $q \in P$, $q \in N_p$ implica $N_q \subseteq N_p$, la familia $\{N_p : p \in P\}$ es base para una topología en P. Sea B el álgebra booleana de conjuntos abiertos regulares en P. Definamos $i : P \to B$ por $i(p) = int(\overline{N_p})$ para cada $p \in P$. Entonces, para cualesquiera $p, q \in P$ se tiene que $p \leq q$

implica $i(p) \leq i(q)$ (es decir, $i(p) \cdot i(q) = i(p)$) y si p es incompatible a q, entonces $i(p) \cdot i(q) = 0$. En efecto, $i(p) \cdot i(q) = 0$ si y sólo si

$$int(\overline{N_p}) \cap int(\overline{N_q}) = \emptyset,$$

que es equivalente a $N_p \cap N_q = \emptyset$ y que a su vez es equivalente a que p sea incompatible con q.

Ahora, si $U \in B \setminus \{0\}$ y $p \in U$; entonces $int(\overline{N_p}) \subseteq U$. Entonces $i(p) \subseteq U$ o bien $i(p) \leq U$. Por lo tanto, $i(P)$ es denso en $B \setminus \{0\}$.

Sea $\mathcal{D} = \{D_\alpha : \alpha < \kappa\}$ una familia de conjuntos densos en P. Entonces,

$$\mathcal{D}' = \{i(D_\alpha) : \alpha < \kappa\}$$

es una familia de conjuntos densos en $B \setminus \{0\}$.

Ahora, $B \setminus \{0\}$ satisface la *c.c.c.* puesto que P la satisface y $i(P)$ es denso en $B \setminus \{0\}$. Para cada $(p, q) \in P \times P$, sea $H_{p,q}$ el conjunto de todos los $r \in P$ tales que o bien $r \leq p$ y $r \leq q$ o r es incompatible con p o r es incompatible con q. Veamos que para cada $(p, q) \in P \times P$, $H_{p,q}$ es denso en P. Si $r \in P$ y r tiene una extensión r' incompatible con p o con q, entonces $r' \in H_{p,q}$ y $r' \leq r$. Si por el contrario no existe tal r', entonces en particular r es compatible con p y así existe $r_1 \in P$ tal que $r_1 \leq r$ y $r_1 \leq p$; pero necesariamente también r_1 es compatible con q y así existe $r_2 \in P$ tal que $r_2 \leq r_1$ y $r_2 \leq q$. Puesto que $r_2 \leq p$ se tiene que $r_2 \in H_{p,q}$ y $r_2 \leq r$.

Nuevamente $i(H_{p,q})$ es denso en $B \setminus \{0\}$. Sea

$$\mathcal{H} = \mathcal{D}' \cup \{i(H_{p,q}) : (p, q) \in P \times P\}.$$

Entonces $|\mathcal{H}| \leq \kappa$ y usando $\mathbf{AM}^b_\kappa$ se infiere la existencia de un filtro $\mathcal{H}$-genérico F en $B \setminus \{0\}$.

Sea $G = i^{-1}(F)$. Entonces para cada $\alpha < \kappa$, $G \cap D_\alpha \neq \emptyset$ y para cada $(p, q) \in P \times P$, $G \cap H_{p,q} \neq \emptyset$. Más aún, G es un filtro en P porque si $p \in G$ y $q \in P$ es tal que $q \geq p$, entonces trivialmente $q \in G$. Además, si $p, q \in G$, como $G \cap H_{p,q} \neq \emptyset$, existe un $r \in G \cap H_{p,q}$ y dado que $i(p)$, $i(q)$, $i(r) \in F$ necesariamente p, q y r son compatibles y así $r \leq p$ y $r \leq q$. Por lo tanto, existe una extensión común a p y q en G. Consecuentemente, G es un filtro $\mathcal{D}$-genérico en P. ■

Para nuestro último teorema necesitaremos introducir el espacio de Stone asociado a un álgebra booleana. Si B es un álgebra booleana, por el Teorema de Representación de Stone (Ejemplo 8.57) existe un homomorfismo (de álgebras booleanas) $\Phi : B \to \mathcal{P}(\mathcal{S}(B))$, donde

$$\mathcal{S}(B) = \{U \subseteq B : U \text{ es un ultrafiltro en } B\}$$

y $\Phi(u) = \{U \in \mathcal{S}(B) : u \in U\}$ para cada $u \in B$. El espacio de Stone asociado a B es $\mathcal{S}(B)$ tomando como base para una topología en $\mathcal{S}(B)$ a todos los conjuntos $\Phi(u)$.

Lema 11.42 *$\mathcal{S}(B)$ es un espacio Hausdorff compacto.*

Demostración:

Sean $U, V \in \mathcal{S}(B)$, $U \neq V$. Entonces $U \setminus V \neq \emptyset$, sea $u \in U \setminus V$. A partir de $\Phi(-u) = \mathcal{S}(B) \setminus U$ se sigue que $\Phi(u)$ es un subconjunto abierto y cerrado de $\mathcal{S}(B)$ que contiene a U y no a V. Así, $\mathcal{S}(B)$ satisface el axioma de separación de Hausdorff.

Ahora sea $A \subseteq B$ y supóngase que $\{\Phi(a) : a \in A\}$ es una cubierta de $\mathcal{S}(B)$ sin subcubiertas finitas. Sea $A' = \{-a : a \in A\}$. Entonces para todo $n \in \omega$ y $a_1, \ldots, a_n \in A$,

$$(-a_1) \cdot (-a_2) \cdot \ldots \cdot (-a_n) \neq 0,$$

puesto que de otro modo $\{\Phi(a_k) : 1 \leq k \leq n\}$ sería una subcubierta finita. Sea $F \subseteq B$ tal que $u \in F$ si y sólo si existen $n \in \omega$ y $a_1, \ldots, a_n \in A$ tales que

$$(-a_1) \cdot (-a_2) \cdot \ldots \cdot (-a_n) \leq u.$$

Entonces F es un filtro en B. Por el Teorema 8.55(b), existe $U \in \mathcal{S}(B)$ tal que $A' \subseteq F \subseteq U$. Como $\{\Phi(a) : a \in A\}$ es una cubierta de $\mathcal{S}(B)$, hay un $a \in A$ tal que $U \in \Phi(a)$, es decir, $a \in U$. Se sigue que

$$0 = a \cdot (-a) \in U$$

y esto contradice que U sea un ultrafiltro. Así, $\mathcal{S}(B)$ es compacto. ■

Teorema 11.43 *Para cualquier $\kappa < 2^{\aleph_0}$, las siguientes proposiciones son equivalentes:*

(a) $\mathbf{AM}_\kappa$

(b) $\mathbf{AM}^*_\kappa$

(c) $\mathbf{AM}^b_\kappa$

(d) Para todo espacio topológico compacto Hausdorff que satisface la c.c.c., siempre que $\mathcal{U}$ sea una familia de subconjuntos abiertos densos no vacíos y $|\mathcal{U}| \leq \kappa$, se cumple que $\bigcap \mathcal{U} \neq \emptyset$.

Demostración:

La equivalencia de (a), (b) y (c) ya se ha demostrado y (a) implica (d) es el Teorema 11.34; por lo tanto, basta demostrar (d) implica (c).

Sea B un álgebra booleana completa que satisface la *c.c.c.* y sea

$$\mathcal{D} = \{D_\alpha : \alpha < \kappa\}$$

una familia de conjuntos densos en $B \setminus \{0\}$. Sea $\mathcal{S}(B)$ el espacio de Stone asociado a B. Por el lema anterior, $\mathcal{S}(B)$ es un espacio compacto Hausdorff. Como $\Phi(u) \cap \Phi(v) = \Phi(u \cdot v)$, tenemos que $\Phi(u) \cap \Phi(v) = \emptyset$ si y sólo si $u \cdot v = 0$; por lo tanto, $\mathcal{S}(B)$ satisface la *c.c.c.* porque B la satisface.

Para cada $\alpha < \kappa$, sea $W_\alpha = \bigcup \{\Phi(u) : u \in D_\alpha\}$. Entonces W_α es abierto, no vacío. Además, W_α es denso en $\mathcal{S}(B)$ pues si $\Phi(v)$ es un abierto básico de $\mathcal{S}(B)$, entonces existe $u \in D_\alpha$ tal que $u \leq v$, luego $\Phi(u) \subset \Phi(v)$ y así $W_\alpha \cap \Phi(v) \neq \emptyset$. Por hipótesis,

$$\bigcap \{W_\alpha : \alpha < \kappa\} \neq \emptyset.$$

Sea $G \in \bigcap \{W_\alpha : \alpha < \kappa\}$. Entonces G es un filtro (de hecho un ultrafiltro) $\mathcal{D}$-genérico en $\mathcal{B}$ porque si $\alpha < \kappa$, $G \in W_\alpha$ implica que existe $u \in D_\alpha$ tal que $G \in \Phi(u)$ y por definición de $\Phi(u)$ se tiene que $u \in G$; por lo tanto, $u \in G \cap D_\alpha$. Esto demuestra que (d) implica (c). ■

Apéndice A

Axiomas de Zermelo-Fraenkel

El tratamiento que hemos seguido de la Teoría de Conjuntos dentro de la - axiomática de Zermelo-Fraenkel, ha sido más bien informal. La razón de ello, es la vaga noción de propiedad que aceptamos; para formalizar (sin que esto altere los resultados expuestos) debemos dar a los axiomas una forma precisa, introduciendo las llamadas *fórmulas* y desarrollando a la Teoría Axiomática de Conjuntos dentro del cá lculo de predicados de primer orden. Todos los objetos son conjuntos. Un excelente desarrollo de esto puede encontrarse en el Capítulo 2 de [KM] o el capítulo preliminar de [D_3].

Las fórmulas de la Teoría de Conjuntos son estructuras que parten de las *fórmulas atómicas*

$$x \in y, \qquad\qquad x = y$$

por medio de los conectivos lógicos y los cuantificadores expuestos en la Sección 2.1.

Axioma 1 (de Existencia) *Hay un conjunto que no tiene elementos.*

Axioma 2 (de Extensión) *Si todo elemento de X es un elemento de Y y todo elemento de Y es un elemento de X, entonces $X = Y$.*

Axioma 3 (Esquema de Comprensión) *Sea* **P** *una fórmula. Para cualquier conjunto A hay un conjunto B tal que $x \in B$ si y sólo si $x \in A$ y x satisface la fórmula* **P**.

Axioma 4 (del Par) *Para cualesquiera conjuntos a y b hay un conjunto C tal que $x \in C$ si y sólo si $x = a$ o $x = b$.*

Axioma 5 (de Unión) *Para cualquier conjunto S, existe un conjunto U tal que $x \in U$ si y sólo si $x \in X$ para algún $X \in S$.*

Axioma 6 (del Conjunto Potencia) *Para cualquier conjunto X, existe un conjunto S tal que $A \in S$ si y sólo si $A \subseteq X$.*

Axioma 7 (de Fundación) *En cada conjunto no vacío A existe $u \in A$ tal que u y A son ajenos.*

Axioma 8 (de Infinitud) *Existe un conjunto inductivo.*

Axioma 9 (Esquema de Reemplazo) *Sea* $\mathbf{P}(x, y)$ *una formula tal que para todo* x *existe un único* y *para el cual* $\mathbf{P}(x, y)$ *se satisface.*

Para todo conjunto A*, existe un conjunto* B *tal que, para todo* $x \in A$*, existe* $y \in B$ *para el cual* $\mathbf{P}(x, y)$ *se satisface.*

Axioma 10 (de Elección) *Todo conjunto no vacío tiene una función de elección.*

ZF denota los axiomas 1 a 9. **ZFC** denota **ZF** + el Axioma de Elección.

Apéndice B

Axiomas Bernays-Gödel

En esta axiomatización se consideran dos tipos de objetos: *conjuntos* y *clases.*

Axioma 1 (*de Extensión de Clases*) *Si todo elemento de X es un elemento de Y, y todo elemento de Y es un elemento de X, entonces $X = Y$.*

Axioma 2 *Cualquier conjunto es una clase.*

Axioma 3 *Si $X \in Y$, entonces X es un conjunto.*

Axioma 4 (*del Par*) *Para cualesquiera conjuntos x y y existe un conjunto $\{x, y\}$.*

Axioma 5 (*de Comprensión*) *Si $\mathbf{P}(x, X_1, \ldots X_n)$ es una fórmula donde los únicos parámetros cuantificados son conjuntos, entonces existe una clase Y tal que $x \in Y$ si y sólo si $\mathbf{P}(x, X_1, \ldots X_n)$.*

Axioma 6 (*de Infinitud*) *Hay un conjunto inductivo.*

Axioma 7 (*de Unión*) *Para cualquier conjunto X, $\bigcup X$ es un conjunto.*

Axioma 8 (*del Conjunto Potencia*) *Para cualquier conjunto X, $\mathcal{P}(X)$ es un conjunto.*

Axioma 9 (*de Reemplazo*) *Si una clase F es una función y X es un conjunto, $F(X)$ es un conjunto.*

Axioma 10 (*de Fundación*) *En cada conjunto no vacío X existe $u \in X$ tal que u y X son ajenos.*

Axioma 11 (*de Elección*) *Hay una función F tal que $F(X) \in X$ para cualquier conjunto no vacío X.*

BG denota los axiomas 1 a 10 y **BGC** denota **BG** + el Axioma de Elección.

Puede probarse que si una proposición conjuntista es demostrable en **ZF** o **ZFC**, entonces también es demostrable en **BG**, y respectivamente en **BGC**. Recíprocamente, un teorema de Shoenfield asegura que si una proposición

que involucra únicamente a conjuntos como variables es demostrable en **BG**, entonces ésta también es demostrable en **ZF**. El resultado también puede generalizarse a **BGC** y **ZFC** usando técnicas distintas a las usadas por Shoenfield.

Apéndice C

Axiomas Adicionales

Los trabajos de Gödel y Cohen implican que se puede aumentar como un nuevo axioma para la Teoría de Conjuntos la proposición

$$2^{\aleph_0} = \aleph_1.$$

No obstante, también de los trabajos de Cohen y W. B. Easton se sigue que para cualquier $\aleph_\alpha$ con $cf(\aleph_\alpha) > \aleph_0$, también

$$2^{\aleph_0} = \aleph_\alpha$$

es un posible axioma adicional para la Teoría de Conjuntos. En otras palabras, el método (*forcing*) inventado por Cohen para la construcción de modelos, permite crear modelos para la Teoría de Conjuntos en los cuales hay $\aleph_\alpha$ subconjuntos de números naturales.

Con todo esto, no existen razones lógicas para decidir si aceptamos como un nuevo axioma la Hipótesis del Continuo, otra proposición de la forma $2^{\aleph_0} = \aleph_\alpha$, o simplemente no aceptamos alguna de estas proposiciones. El problema de elegir una de las opciones reside en que no son intuitivamente obvias como los axiomas **ZFC**. Existe peligro que alguna de las opciones nos conduzca a resultados no deseados; como en el caso del Axioma de Elección que tiene consecuencias "paradójicas" (es decir, usándolo podemos obtener resultados que están en conflicto con nuestra intuición; por ejemplo, el Teorema de Banach-Tarski). Sin embargo, la Hipótesis del Continuo, así como la Hipótesis Generalizada del Continuo, tienen importantes aplicaciones tanto en la propia Teoría de Conjuntos (ver Sección 10.5) como en otras ramas de la Matemática. En resumen, dos posibles axiomas adicionales son los siguientes:

HC $2^{\aleph_0} = \aleph_1$.

HGC Para cualquier $\alpha \in \mathbf{Ord}$, $\quad 2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

Además del famoso Axioma de Martin:

AM Si $(P, \leq)$ es un conjunto pre-ordenado que satisface la *c.c.c.* y si $\mathcal{D}$ es una familia de menos que $2^{\aleph_0}$ subconjuntos densos de P, entonces existe un filtro $\mathcal{D}$-genérico en P.

y la Hipótesis de Souslin:

HS No existen líneas de Souslin.

Las implicaciones entre estos axiomas están dadas en el siguiente diagrama.

$$\begin{array}{ccccc} \mathbf{HGC} & \Rightarrow & \mathbf{HC} & \Rightarrow & \mathbf{AM} \\ & & \mathbf{AM} & \Rightarrow & \mathbf{HS} \end{array}$$

Igualmente el grupo de los llamados *axiomas de cardinales grandes* es muy empleado por las valiosas consecuencias que también aportan tanto a la Teoría de Conjuntos como a otras ramas de la Matemática. Aquí formularemos algunas hipótesis que involucran tipos de cardinales grandes que fueron presentados en el Capítulo 10; pero existen otras proposiciones de este tipo que se sabe son tanto independientes como consistentes con los axiomas **ZFC**. Hay otras de las cuales sólo se conoce la consistencia con **ZFC**. La idea para descubrir una de estas hipótesis es la siguiente: Dada $\mathbf{P}(\kappa)$ una propiedad que involucre números cardinales, se investiga cuándo $\mathbf{P}(\kappa)$ o no $\mathbf{P}(\kappa)$ es cierta para alguno, muchos o todos los números cardinales. Algunas veces se descubre que una particular propiedad $\mathbf{P}(\kappa)$, como $\kappa \to (\kappa)^2_2$, es extremadamente extraña y que el mínimo número cardinal que satisface $\mathbf{P}(\kappa)$ es increíblemente grande, tan grande que incluso no es posible demostrar, a partir de los axiomas **ZFC**, que haya un tal cardinal κ. En este caso la proposición "existe un cardinal κ tal que $\mathbf{P}(\kappa)$" es llamada *hipótesis de cardinal grande*, al menos hasta que sea refutada, pues obviamente existe la posibilidad de que $\mathbf{P}(\kappa)$ sea tan restrictiva que suponer la existencia de un κ que satisfaga $\mathbf{P}(\kappa)$ nos lleve a una contradicción. Para que una hipótesis tenga categoría de axioma usualmente se necesita saber si ella es tanto consistente como independiente a **ZFC**.

CI Existen cardinales inaccesibles.

CFI Existen cardinales fuertemente inaccesibles.

CM Existen cardinales medibles.

CdC Existen cardinales débilmente compactos.

CC Existen cardinales compactos.

CMa Existen cardinales de Mahlo.

Las implicaciones que relacionan estos axiomas son las siguientes:

$$\mathbf{CC} \Rightarrow \mathbf{CM} \Rightarrow \mathbf{CdC} \Rightarrow \mathbf{CMa} \Rightarrow \mathbf{CFI} \Rightarrow \mathbf{CI}$$

Una muestra del poder de una de estas hipótesis es la siguiente: Un famoso teorema de Gödel dice que la consistencia de **ZFC** no pude demostrarse a partir de **ZFC**; sin embargo, sí puede ser demostrada a partir de la unión de **ZFC** y **CI** (que denotamos por **ZFC + CI**).

Por otro lado, **CI** está lejos de ser lo suficientemente fuerte como para dar solución incluso a los problemas más clásicos de la Teoría de Conjuntos, pero las demostraciones de independencia en **ZFC** mantienen su validez en **ZFC + CI.**

Otra consecuencia de **CI** es que el continuo puede ser extremadamente grande. Ya comentamos que el trabajo de Cohen deja abierta la posibilidad de que $2^{\aleph_0} = \aleph_{16}$ o $2^{\aleph_0} = \aleph_{\omega_1}$; sin embargo, la consistencia de **ZFC + CI** es equivalente a la consistencia de **ZFC** + "$2^{\aleph_0}$ es débilmente inaccesible", y equivalente a la consistencia de **ZFC** + "$\exists \kappa < 2^{\aleph_0}$ tal que κ es débilmente inaccesible". También, si **ZFC + CI** es consistente, así es **ZFC + HGC**.

Mencionamos ahora otro resultado interesante que tiene relación con la existencia de un cardinal grande. Si hay un cardinal medible, entonces cualquier conjunto de números reales que es la imagen continua del complemento de una imagen continua de un conjunto de Borel, es medible. Es ciertamente sorpresivo que la existencia de un cardinal grande implique la medibilidad de un conjunto de números reales.

Otro grupo de hipótesis importantes es el conocido como *principios combinatorios*. No daremos aquí ni siquiera una idea de cómo éstos surgen, además de que naturalmente, no es propósito de este apéndice hacer una amplia lista de ellos; los que enunciamos se encuentran entre los más famosos y que han demostrado ser de gran utilidad.

$\diamondsuit$ Existen conjuntos $A_\alpha \subseteq \alpha$, para $\alpha < \omega_1$, tales que para cada $A \subseteq \omega_1$, el conjunto $\{\alpha : \omega_1 : A \cap \alpha = A_\alpha\}$ es estacionario.

$\diamondsuit^+$ Existen conjuntos $\mathcal{A}_\alpha \subseteq \mathcal{P}(\alpha)$, para $\alpha < \omega_1$, tales que $|\mathcal{A}_\alpha| \leq \aleph_0$ y para $A \subseteq \omega_1$, existe un conjunto cerrado y no acotado $C \subseteq \omega_1$ tal que

(a) para cualquier $\alpha \in C$, $A \cap \alpha \in \mathcal{A}_\alpha$, y

(b) para cualquier $\alpha \in C$, $C \cap \alpha \in \mathcal{A}_\alpha$.

HK Existe una familia $\mathcal{F} \subseteq \mathcal{P}(\omega_1)$ tal que $|\mathcal{F}| \geq \aleph_2$ y para cualquier $\alpha < \omega_1$, $|\{A \cap \alpha : A \in \mathcal{F}\}| < \aleph_1$.

□ Existe un conjunto $\{C_\alpha : \alpha < \omega_2,\ \alpha \text{ ordinal límite}\}$ tal que

(a) C_α es un subconjunto cerrado y no acotado de α,

(b) si $\beta < \alpha$ y $C_\alpha \cap \beta$ es cofinal en β, entonces $C_\beta = C_\alpha \cap \beta$, y

(c) si $cf(\alpha) \leq \aleph_0$, entonces $|C_\alpha| \leq \aleph_0$.

Algunas de las implicaciones existentes son las siguientes:

$$\begin{array}{ccccc} \diamondsuit^+ & \Rightarrow & \diamondsuit & \Rightarrow & \mathbf{HC} \\ \Downarrow & & \Downarrow & & \\ \mathbf{HK} & & \neg\mathbf{HS} & & \end{array}$$

Este apéndice de axiomas adicionales para la Teoría de Conjuntos no puede finalizar sin el estelar *Axioma de Constructibilidad*. La noción de constructibilidad en Teoría de Conjuntos fue introducida por Gödel en 1938 para demostrar la consistencia del Axioma de Elección y de la Hipótesis Generalizada del Continuo con los axiomas **ZF** y **ZFC**, respectivamente. La motivación para la noción de constructibilidad es más o menos como sigue. Trabajando con los axiomas **ZF**, el universo **V** de todos los conjuntos se "obtiene" comenzando con el conjunto vacío $\emptyset$ e iterando la operación de tomar conjunto potencia. De esta manera se obtiene la jerarquía acumulativa:

$$\begin{aligned} V_0 &= \emptyset \\ V_\alpha &= \bigcup \{\mathcal{P}(V_\beta) : \beta < \alpha\}. \end{aligned}$$

Y entonces tenemos

$$\mathbf{V} = \bigcup_{\alpha \in \mathbf{Ord}} V_\alpha.$$

La razón de por qué ciertas cuestiones sobre la jerarquía acumulativa no son contestables con **ZF** o **ZFC** es el hecho de que la noción de conjunto potencia es bastante vaga; sabemos que $\mathcal{P}(X)$ es el consiste de *todos* los subconjuntos de X; pero ¿qué significa aquí *todos*? El *universo constructible,* **L**, se obtiene al "hacer preciso" el significado de *todos* y tomar, para cualquier conjunto A, al conjunto potencia de A lo más pequeño posible, sin contradecir a los demás axiomas. A los conjuntos que integran **L** se les llama *conjuntos construibles.* El Axioma de Constructibilidad postula que **V** es igual a **L**.

Axioma de Constructividad Todo conjunto es construible.

Este extraño axioma es una herramienta fundamental para la investigación dentro de la Teoría de Conjuntos. Por ejemplo, tres importantes consecuencias de $\mathbf{V} = \mathbf{L}$ son: el Axioma de Elección, **HGC** y $\diamondsuit^+$.

Bibliografía

[A_1] P. Aczel. *Non-Well-Founded Sets.* Center for the Study of Language and Information, 1988.

[A_2] J. A. Amor Montaño. *Conceptos y resultados básicos de conjuntos*. Vínculos Matemáticos, Departamento de Matemáticas. Facultad de Ciencias, U.N.A.M., 1992.

[AKN] H. Andréka, A. Kurucz, I. Németi. *Conections between axioms of set theory and basic theorems of universal algebra.* J. Symb. Logic **59** (1994) 912-923.

[A_3] T. M. Apostol. *Calculus*. Volume 1, Second Edition. John Willey & Sons, 1967.

[B_1] P. Bernays. *A system of axiomatic set theory*. J. Symb. Logic **2** (1935) 65-77; **6** (1941) 1-17, 133-145; **7** (1942) 65-89; **8** (1943) 89-106; **13** (1948) 65-79; **19** (1954) 81-96.

[BF] J. L. Bell, D. F. Fremlin. *A geometric form of the Axiom of Choice*. Fund. Math. **77** (1972) 167-170.

[BT] R.L. Blair, M.L. Tomber. *The axiom of choice for finite sets*, Proc. Amer. Math. Soc **11** (1960) 222-226.

[B_2] A. Blass. *A model without ultrafilters.* Bull. Acad. Polon. Sci. **25** (1977) 329-331.

[B_3] N. Bourbaki. *Elements of Mathematics. Theory of Sets.* Addison-Wesley, 1968.

[B_4] N. Bourbaki. *Elementos de Historia de las Matemáticas*. Alianza - Editorial, 1972.

[B_5] N. Brunner. *The axiom of choice in topology.* Notre Dame J. Formal Logic **24** (1983) 305-317.

[C_1] G. Cantor. *Beiträge zur Begründung der transfiniten Mengenlehre.* Math. Ann. **46** (1895) 481-512.

[C_2] G. Cantor. *Grsammelte Abhandlungen mathematischen und philosophischen Inhalts*, edited by Zermelo 488, 1932.

[C_3] G. Cantor. *Contributions to the founding of the theory of Transfinite Numbers.* Dover, 1955.

[C_4] P. J. Cohen. *The independence of the continuum hypothesis.* Proc. Nat. Acad. Sci. U.S.A. **50** (1963) 1143-1148; **51** (1964) 105-110.

[C_5] W. W. Comfort. *A theorem of Stone-Čech type, and a theorem of Tychonoff type, without the Axiom of Choice; and their realcompact analogues.* Fund. Math. **63** (1968) 97-110.

[CN] W. W. Comfort, S. Negrepontis. *The Theory of Ultrafilters.* Springer-Verlag, 1974.

[C_6] T. Coquand. *An intuitionistic proof of Tychonoff's theorem.* J. Symb. Logic. **57** (1992) 28-32.

[D_1] J. W. Dauben. *Georg Cantor. His Mathematics and Philosophy of the Infinite.* Princeton Univ. Press, 1979.

[D_2] R. Dedekind. *Was sind und was sollen die Zahlen?* Vieweg, Braunschweig, 1888.

[D_3] K. J. Devlin. *Constructibility.* Handbook of Mathematical Logic (Ed. J. Barwise). North-Holland Pub. Co., 1977. 453-490.

[D_4] K. Devlin. *The Joy of Sets.* Springer-Verlag. Second Edition,1993.

[D_5] J. Dugundji. *Topology.* Allyn and Bacon, 1966.

[E] W. B. Easton. *Powers of regular cardinals.* Annals of Mathematical Logic **1** (1970) 491-502.

[E_1] H. B. Enderton. *Elements of Set Theory.* Academic Press, 1977.

[F_1] A. A. Fraenkel. *Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre.* Math. Ann. **86** (1922) 230-237.

[F_2] S. Feferman. *Some applications of the notions of forcing and the generic sets.* Fund. Math. **56** (1964) 325-345.

[F_3] G. Frege. *Die Grundlagen der Arithmetik* (Loebner, Breslau 1884).

[F_4] G. Frege. *Grundgesetze der Arithmetik,* vol. 2 (Pohle, Jena 1903).

[G_1] M. Glazman. *Conjuntos.* Vínculos Matemáticos, Departamento de Matemáticas, Facultad de Ciencias, U.N.A.M., 1993.

[G_2] K. Gödel. *The consistency of the Axiom of Choice and of the Generalized Continuum Hypothesis*. Proc. Nat. Acad. Sci. **24** (1938). Annals of Math. Studies **3**, 1951.

[G_3] A. R. Grainger. *Flat Sets.* J. Symb. Logic **59** (1994) 1012-1021.

[G_4] I. Grattan-Guinness. *Del Cálculo a la Teoría de Conjuntos 1630-1910. Una introducción histórica.* Alianza Universidad, 1984.

[H_1] P. R. Halmos. *Naive Set Theory.* Springer-Verlag, 1974.

[H_2] P. R. Halmos. *Measure Theory.* Springer-Verlag, 1974.

[H_3] J. D. Halpern. *The independence of the axiom of choice from the Boolean prime ideal theorem*, Fund. Math. **55** (1964) 57-66

[H_4] F. Hausdorff. *Der potenzbegriff in der Mengenlehre.* Jahr. Deutsch. Math. Ver. **13** (1904).

[H_5] F. Hausdorff. *Set Theory.* Chelsea Publishing Company, Second Edition, 1957.

[HS_1] E. Hewitt, K. Stromberg. *Real and Abstract Analysis.* Springer-Verlag, 1965.

[HS_2] H. Herrlich, G. E. Strecker. *Category Theory: an introduction.* Allyn and Bacon, 1973.

[HJ] K. Hrbacek, T. Jech. *Introduction to Set Theory.* Marcel Dekker Inc., Second Edition, 1978.

[J_1] N. Jacobson. *Basic Algebra I y II.* W. H. Freeman, Second Edition, 1985.

[J_2] T. Jech. *The Axiom of Choice*. North-Holland Pub. Co., 1973.

[J_3] T. Jech. *Set Theory.* Academic Press, 1978.

[K_1] E. Kamke. *Theory of Sets.* Dover, 1950.

[K_2] J. L. Kelley. *The Tychonoff product theorem implies the Axiom of Choice*. Fund. Math. **T-37** (1950) 75-76.

[K_3] J. L. Kelley. *General Topology*. Springer-Verlag, 1955.

[K_4] K. Kunen. *Combinatorics*. Handbook of Mathematical Logic (Ed. J. Barwise). North-Holland Pub. Co., 1977. 371-402.

[K_5] K. Kunen. *Set Theory. An introduction to Independence Proofs*. North Holland, 1980.

[K_6] K. Kuratowski. *Sur la notion de l'ordre dans la théorie des ensembles*. Fund. Math. **2** (1921) 167-171.

[KM] K. Kuratowski, A. Mostowski. *Set Theory and Logic*. Studies in Logic and Foundations of Mathematics, North-Holland, 1968.

[L_1] E. Landau. *Foundations of Analysis.* Chelsa Publishing, Third Edition, 1966.

[L_2] S. Lang. *Algebra*. Addison-Wesley Pub., Third Edition, 1993.

[L_3] H. Läuchli. *Auswahlaxiom in der algebra.* Commentarii Math. Helvetici **37** (1962-63) 1-18.

[L_4] S. Lipschutz. *Teoría de Conjuntos y Temas Afines.* Schaum, McGraw-Hill, 1991.

[L_5] P. A. Loeb. *A new proof of the Tychonoff's theorem.* Amer. Math. Monthly **72** (1965) 711-717.

[L_6] M. López Mateos. *Los Conjuntos*. Comunicaciones Internas, Departamento de Matemáticas, Facultad de Ciencias, U.N.A.M., 1978.

[LR] J. Łós, C. Ryll-Nardzrwski. *Effectiveness of the representation theory of Boolean algebras.* Fund. Math. 41 (1955) 49-56.

[M_1] S. Mac Lane. *Categories for the Working Mathematician*. Springer-Verlag, Third Printing, 1971.

[M_2] D. Mirimanoff. *Les antinomies de Russell et de Burali-Forti et le probleme fondamental de la théorie des ensembles*. Enseig. Math. **19** (1917) 37-52.

[M_3] G. H.. Moore. *Zermelo's axiom of choice: its origins development, and influence.* Studies in the History of Mathemnatics and Physical Sciences **8** (1982) Springer-Verlag.

[M_4] R. L. Moore. *Foundations of Point Set Theory.* Am. Math. Soc. Colloquium Publ. XIII, 1932.

[M_5] A. P. Morse. *A Theory of Sets.* Academic Press, Second Edition, 1968.

[N_1] J. von Neumann. *Zur Einführung der transfiniten Zahlen.* Ac. Sci. Hung. **1** (1923).

[N_2] J. von Neumann. *Eine Axiomatisierung der Mengenlehre.* Crelle J. **154** (1925) 219-240.

[N_3] J. von Neumann. *Die Axiomatisierung der Mengenlehre.* Math. Z. **27** (1928) 699-752.

[P_1] G. Peano. *Arithmeties Principia.* Bocca, Turin. 1889.

[P_2] G. Peano. *Formulaire de Mathématiques.* (Torino 1895) 144.

[P_3] G. Peano. *Sulla denizione di funzione.* Atti Real Ac. Lin. **20** (1911) 3-5.

[P_4] C. C. Pinter. *Set Theory.* Addison-Wesley, 1971.

[P_5] M. D. Potter. *Sets: an introduction.* Oxford Science Publications, 1990.

[P_6] I. Puga. *Teoría de Conjuntos.* Comunicaciones Internas, Departamento de Matemáticas, Facultad de Ciencias, U.N.A.M., 1989.

[R_1] J. Roitman, *Introduction to Modern Set Theory.* John Willey & Sons, 1990.

[R_2] J. E. Rubin. *Set Theory for the Mathematician.* Holden-Day, 1968.

[RR] H. Rubin, J. E. Rubin. *Equivalents of the Axiom of Choice, II.* North-Holland, 1985.

[R_3] M. E. Rudin. *Martin's axiom.* Handbook of Mathematical Logic (Ed. J. Barwise). North-Holland Pub. Co., 1977. 491-502.

[R_4] B. Russell. *Introducción a la Filosofía Matemática.* Paidos, 1988.

[S_1] Z. Samadeni. *Periods of measurable functions and the Stone-Čech compactification.* Amer. Math. Monthly **71** (1964) 891-893.

[S_2] P. Samuel. *Los Universos y la estructura de los conjuntos.* Revista Matemática, No. XVI (1964) 23-33.

[S_3] D. Scott. *The theorem on maximal ideals in lattices and the axiom of choice.* Bull. Am. Math. Soc. (1954) **60** 83.

[S_4] D. Scott. *Prime ideals theorems for rings, lattices and Boolean algebras.* Bull. Am. Math. Soc. (1954) **60** 390.

[S_5] J. R. Shoenfield. *Axioms of set theory.* Handbook of Mathematical Logic (Ed. J. Barwise). North-Holland Pub. Co., 1977. 321-344.

[S_6] T. Skolem. *Untersuchungen über die Axiome des Klassenkalküls....* Skrifter utgit av Videnskapsselkapet i Kristiania, I Klasse **3** (Oslo 1919).

[S_7] T. Skolem. *Einige Bemerkungen zur axiomatischen Bergründung der Mengenlehre.* Wissenchaftliche Vortrage gehalten auf dem fünften Kongress der Skandinavischen Matematiker in Helsingfors (1922) 217-232.

[S_8] E. Specker. *The axiom of choice in Quine's 'New foundations for mathematical logic'.* Proc. Natl. Acad. Sci. U.S.A. **39** (1953) 972-975.

[S_9] M. Spivak. *Calculus.* Segunda Edición, Repla, 1988.

[S_{10}] R. R. Stoll. *Set Theory and Logic.* Dover, 1979.

[T] A. Tarski. *Prime ideal theorems... .* Bull. Am. Math. Soc. (1954) **60** 390-391.

[V] G. Vitali. *Sul problema della misura del gruppi di punti di una retta.* (Bologna 1905).

[W_1] S. Wagon. *The Banach-Tarski Paradox.* Cambridge University Press, 1987.

[W_2] J. D. Weston. *A generalization of Ascoli's theorem.* Mathematika **6** (1959) 19-24.

[W_3] E. S. Wolk. *On theorems of Tychonoff, Alexander and R. Rado*, Proc. Amer. Math. Soc. **18** (1967) 113-115.

[Z_1] E. Zermelo. *Beweiss dass jade Menge wohlgeordnet werden kann.* Math. Ann. **59** (1904) 514-516.

[Z_2] E. Zermelo. *Untersuchungen über die Grundlagen der Mengenlehre I.* Math. Ann. **65** (1908) 261-281.

[Z_3] M. Zorn. *A remark on method in transfinite algebra.* Bull. Am. Math. Soc. **41** (1935) 667-670.

.

Índice

A

Alas, O. T., 193
aleph, 248
    cero, 169
álgebra
    booleana, 199
    booleana completa, 313
    de conjuntos, 204
algoritmo de la división, 118
Andenaes, P. R., 192
Andréka, H., 18
anillo $\mathcal{P}(X)$, 28
árbol, 288
axioma
    débil de existencia, 22
    débil de unión, 22
    débil del conjunto potencia, 22
    débil del par, 22
    de comprensión, 321
    de constructividad, 326
    de elección, 177, 320
    de elección n-finito, 212
    de elección dependiente, 211
    de elección para conjuntos finitos, 212
    de elecciones numerables, 210
    de existencia, 10, 319
    de extensión, 10, 319, 321
    de fundación, 18, 319, 321
    de infinitud, 102, 320
    de Martin, 303
    de reemplazo, 321
    de unión, 15, 319
    del conjunto potencia, 17, 319
    del Par, 319
    esquema de comprensión, 12, 319
    esquema de reemplazo, 223, 320
Axiomas
    de Bernays-Gödel, 321
    de cardinales grandes, 324
    de Peano, 117
    de Zermelo-Fraenkel, 319

B

Banach, S., 281, 286
bases de Hamel, 190
Bell, L. J., 192
Bernays, P. A., 5, 181, 210
Blass, A., 190, 204
Bolzano, B., 2

C

cálculo
    de longitud α, 229
    de longitud m, 107
cadena, 80
campo ordenado, 206
Cantor, G., 1–4, 170, 186, 218, 297
carácter de un álgebra booleana, 208
cardinal
    compacto, 290
    débilmente compacto, 289
    débilmente de Mahlo, 292
    débilmente inaccesible, 270
    de Hausdorff, 293
    de Mahlo, 292
    de Ramsey, 293
    fuertemente inaccesible, 279
    límite, 268
    límite fuerte, 278

medible, 287
regular, 267
secesor, 268
singular, 267
clase, 13
de equivalencia, 70
clausura, 188
algebraica, 191
co-núcleo, 208
cofinalidad de α, 270
Cohen, P. J., 171, 178, 323
complemento, 29
respecto de ..., 26
condición de la cadena contable, 300, 302
conectivos lógicos, 8
conjunto
a lo más numerable, 156
acotado, 109
bien ordenado, 85
cerrado y no acotado, 290
cociente, 71
completo, 299
de índices, 35
de Cantor, 66
de representantes, 72
definición de Cantor, 1
delgado, 291
denso, 173, 297
denso en ..., 299
estacionario, 291
finito, 113, 150
finito según Dedekind, 164
inductivo, 101
infinito, 150
infinito según Dedekind, 164
medible según Lebesgue, 189
numerable, 156
ordenado, 77
potencia, 17
pre-ordenado, 301
separable, 300
singular o unitario, 14
transitivo, 98
vacío, 11
conjuntos ajenos, 24
conjuntos equipotentes, 96
conjuntos hereditariamente finitos, 226
continuación de conjuntos bien ordenados, 184
continuidad secuencial, 188
cordenada, 30
cortadura de Dedekind, 299
cota
inferior, 81
superior, 81
cuantificadores, 9

D

Dedekind, R., 2–4, 118
diferencia de conjuntos, 25
diferencia simétrica, 27

E

Easton, W. B., 323
elemento, 10
mínimo, 80
máximo, 80
maximal, 80
minimal, 80
elementos comparables, 79
espacio de Stone, 316
espectro de un álgebra Booleana, 208

F

familia
f-inductiva, 182

ajena por pares, 40
casi ajena, 305
de carácter finito, 181
de conjuntos, 15
indizada, 35
indizada de conjuntos, 65
Feferman, S., 204, 214
Felgner, U., 191
filtro, 201
κ-completo, 286
$\mathcal{D}$-genérico, 303
cerrado y no acotado, 290
principal, 202
sobre un conjunto, 192
fórmula
de Bernstein, 278
de Hausdorff, 278
fórmulas, 319
Fraenkell, A. A., 224
Frege, G., 69, 99
Fremlin, D. H., 192
función, 49
biyectiva, 55
característica, 50
composición, 53
constante, 50
continua, 147, 290
coordenada, 62, 68
creciente, 86
de elección o selectora, 177
de Hartog, 256
decreciente, 86
extensión, 52
identidad, 50
inclusión, 50
indizadora, 65
inversa, 56
inversa derecha, 58
inversa izquierda, 58
invertible, 55
inyectiva, 55
normal, 290
proyección, 50, 66
proyección natural, 73
que preserva relaciones, 73
restricción, 52
sobreyectiva, 55
vacía, 53
funciones compatibles, 60

G
Gödel, K., 5, 170, 178, 323, 325

H
Halpern, J. D., 193, 203
Hausdorff, F., 27, 43, 79, 186, 269
Hilbert, D., 170, 186
hipótesis
de cardinal grande, 324
de Souslin, 300
del continuo, 170
generalizada del continuo, 273

I
ideal, 200
κ-completo, 286
primo, 200
principal, 200
ínfimo, 81
intersección, 23
de una familia, 35
intervalo cerrado, 91
isomorfismo
entre álgebras booleanas, 205
entre conjuntos ordenados, 84

J
Jech, T., 300
Jensen, R. B., 301

K
Kakutani, S., 193
Kelley, J. L., 20, 193
Klimovski, G., 191
Kneser, H., 195
Kronecker, L., 3
Kunen, K., 301
Kuratowski, K., 31, 187, 281, 286
Kurucz, A., 18

L
Läuchli, H., 194
límite
    inferior de una familia, 40
    superior de una familia, 40
línea de Souslin, 300
Landau, E., 142
Leibniz, G. W. von, 49
lema
    de Kuratowski-Zorn, 183
    de Tukey-Teichmüller, 182
    de Urysohn, 194
Lembcke, J., 192
Levy, A., 195
leyes de De Morgan, 26
límite
    de una sucesión creciente de ordinales, 266
Lindenbaun, A., 273
Los, J., 193, 207
Luxemburg, W. A. J., 207

M
Mahlo, P., 292
Martin, D. A., 301
mayor entero, 145
medida
    σ-aditiva, 281
    2-valuada, 286
miembro, 10
Mirimanoff, D., 20, 224
modelo, 214
Morse, A. P., 20

N
Németi, I., 18
número
    algebraico, 160
    cardinal, 246
    de Hartog, 247, 259
    de Hartog de un cardinal, 257
    entero, 122
    natural, 98
    ordinal, 218
    racional, 127
    real, 138
    trascendental, 160
Neumann, J. von, 4, 5, 20, 99, 224
notación de flecha, 292
núcleo, 208

O
operación binaria, 111
orden
    de yuxtaposición, 89
    dual, 89
    estricto, 78
    inducido, 89
    lexicográfico horizontal, 79
    lexicográfico vertical, 79
    lineal o total, 79
    parcial, 77
    pre-, 78, 301
    producto, 90
ordinal
    inicial, 246
    límite, 219
    sucesor, 219

P

par
- no ordenado, 14
- ordenado, 30

paradoja, 1
paradoja de Russell, 13
partición, 71
Peano, G., 10, 17, 118
pre-orden, 301
principio
- de extensión de orden, 206
- de inducción, 103
- de inducción transfinita, 227
- maximal de Hausdorff, 183

principios combinatorios, 325
producto cartesiano, 31
- de una familia, 65

propiedad, 8
- arquimediana, 130, 140
- de densidad, 139
- de la intersección finita, 202
- de la máxima cota inferior, 91
- de la mínima cota superior, 91

Q

Quine, W. V., 20

R

relación
- antisimétrica, 77
- asimétrica, 78
- binaria, 44
- campo de una, 45
- composición, 47
- de congruencia módulo n, 71
- de equivalencia, 69
- de inclusión, 45
- de orden, 77
- de pertenencia, 47
- diferencia, 44
- dominio de una, 45
- identidad, 44
- imagen de una, 45
- imagen inversa de una, 45
- inversa, 46
- rango de una, 45
- reflexiva, 69
- simétrica, 69
- transitiva, 69
- vacía, 44

representación decimal, 145
representante, 176
retícula, 90
Russell, B., 4, 13, 20, 99, 186
Ryll-Nardzewski, C., 193, 207

S

σ-completitud, 286
Samadeni, Z., 204
Schwarz, H. M., 3
segmento inicial, 85
Sierpiński, W., 180, 195, 204, 273, 279
sistema
- de conjuntos, 15
- de funciones compatibles, 60

Skolem, T., 20, 224
Solovay, R. M., 301
Specker, E., 20, 273
Spivak, M., 142
subconjunto, 16
- propio, 78

sucesión, 112
- de Cauchy, 132, 142
- de Fibonacci, 109
- finita, 112
- límite de una, 142
- semiconstante, 160
- transfinita, 228
- transfinita creciente, 266

sucesor de un conjunto, 101
sucesor inmediato, 86
supremo, 81
    de un conjunto de ordinales, 220
Szele, T., 195

T
Tarski, A., 273, 279, 286, 287
Teichmüler, O., 187
Tennenbaum, S., 300, 301
teorema
    de Artin-Schreir, 206
    de Banach-Tarski, 195
    de Cantor, 163
    de Cantor-Schröder-Bernstein, 162
    de Hahn-Banach, 191, 207
    de Hartog, 257
    de Hausdorff, 195
    de König, 264
    de Nielson-Schreir, 190
    de recursión, 106
    de recursión generalizada, 225
    de recursión paramétrica, 108
    de recursión transfinita, 229
    de recursión transfinita paramétrica, 231
    de representación de Stone, 205
    de Tarski, 258
    de Tychonoff, 192
    del buen orden, 185
    del ideal primo, 203
    del ultrafiltro, 204
    del valor intermedio (ejercicio 9), 147
    fórmula de Bernstein, 278
    fórmula de Hausdorff, 278
terna
    no ordenada, 16
    ordenada, 30
tipo de orden, 225
Tukey, J. W., 187

U
Ulam, S., 286, 287
ultrafiltro, 202
unión, 23
    ajena, 34
    de una familia, 35
unicidad del campo de los números reales, 142

V
Vitali, G., 73, 189

W
Ward, L. E., 181, 193
Weiestrass, K. W. T., 3
Whitehead, A. N., 20

Z
Zermelo, E., 4, 175, 186, 224
Zorn, M., 187, 190